Tivoli Public Key Infrastructure

RA Desktop

Version 3 Release 7.1

SH12-2977-02

Tivoli Public Key Infrastructure

RA Desktop

Version 3 Release 7.1

SH12-2977-02

Copyrightvermerke

Copyright © 1999, 2001 IBM Corp., einschließlich dieser Dokumentation und aller Software. Alle Rechte vorbehalten. Kann nur gemäß der Softwarelizenzvereinbarung von Tivoli Systems bzw. IBM oder dem Anhang für Tivoli-Produkte der IBM Nutzungsbedingungen verwendet werden. Diese Veröffentlichung darf ohne vorherige schriftliche Genehmigung der IBM Corp. weder ganz noch in Auszügen auf irgendeine Weise - elektronisch, mechanisch, magnetisch, optisch, chemisch, manuell u. a. - vervielfältigt, übertragen, aufgezeichnet, auf einem Abrufsystem gespeichert oder in eine andere Computersprache übersetzt werden. Die IBM Corp. gestattet Ihnen in begrenztem Umfang, eine Hardcopy oder eine Reproduktion einer maschinenlesbaren Dokumentation für den eigenen Gebrauch zu erstellen, unter der Voraussetzung, dass jede dieser Reproduktionen mit dem Copyrightvermerk der IBM Corp. versehen ist. Weitere das Copyright betreffende Rechte werden nur nach vorheriger schriftlicher Genehmigung durch die IBM Corp. gewährt. Die Veröffentlichung dient nicht zu Produktionszwecken. **Die in diesem Dokument aufgeführten Beispiele sollen lediglich zur Veranschaulichung und zu keinem anderen Zweck dienen.**

Marken

AIX, DB2, DB2 Universal Database, IBM, RS/6000, SecureWay, Tivoli and WebSphere sind in gewissen Ländern eingetragene Marken der International Business Machines Corp. oder von Tivoli Systems Inc.

Das Programm Tivoli PKI (im folgenden als ″Programm″ bezeichnet) enthält Komponenten von IBM WebSphere Application Server und IBM HTTP Web Server (″IBM Server″). Diese dürfen nur zusammen mit dem Programm installiert und entsprechend der für das Programm geltenden Lizenzvereinbarungen in Kombination mit diesem verwendet werden. Die IBM Server müssen auf derselben Maschine wie das Programm installiert sein. Sie sind nicht berechtigt, sie unabhängig vom Programm zu installieren und zu verwenden.

Das Programm Tivoli PKI (im folgenden als ″Programm″ bezeichnet) enthält Komponenten von DB2 Universal Database. Diese Komponenten dürfen nur zusammen mit dem Programm installiert und entsprechend der für das Programm geltenden Lizenzvereinbarungen in Kombination mit diesem verwendet werden, um Daten zu speichern und zu verwalten, die vom Programm verwendet oder generiert werden. Für andere Datenverwaltungsoperationen ist der Einsatz nicht gestattet. Diese Lizenz gilt z. B. nicht für eingehende Verbindungen zur Datenbank, die von anderen Anwendungen aus für Abfragen und Berichtserstellungsoperationen hergestellt werden. Sie sind lediglich zur Installation und Verwendung dieser Komponenten auf der gleichen Maschine berechtigt, auf der auch das Programm installiert und verwendet wird.

Das Programm enthält Komponenten des IBM WebSphere Application Server und des IBM HTTP Web Server (″IBM Server″). Sie sind nicht berechtigt, die IBM Server zu anderen Zwecken als in Verbindung mit der lizenzgerechten Verwendung des Programms zu benutzen. Die IBM Server müssen auf derselben Maschine wie das Programm installiert sein. Sie sind nicht berechtigt, sie unabhängig vom Programm zu installieren und zu verwenden.

Java und alle auf Java basierenden Marken und Logos sind in gewissen Ländern Marken der Sun Microsystems, Inc.

Microsoft, Windows, Windows NT und das Windows-Logo sind in gewissen Ländern Marken der Microsoft Corporation.

UNIX ist eine eingetragene Marke und wird ausschließlich von der X/Open Company Limited lizenziert.

Pentium ist in gewissen Ländern eine Marke der Intel Corporation.

Dieses Programm enthält Sicherheitssoftware von RSA Data Security, Inc. Copyright © 1994 RSA Data Security, Inc. Alle Rechte vorbehalten.

Dieses Programm enthält STL-Software (STL = Standard Template Library) von Hewlett-Packard Company. Copyright (c) 1994.

- Die Berechtigung zum Verwenden, Kopieren, Ändern, Verteilen und Verkaufen dieser Software sowie der zugehörigen Dokumentation für die gewünschten Zwecke wird hiermit gebührenfrei erteilt. Voraussetzung hierfür ist allerdings, daß der o. a. Copyrightvermerk auf allen Kopien erscheint, und daß sowohl dieser Copyrightvermerk als auch dieser Berechtigungshinweis in der zugehörigen Dokumentation aufgeführt werden. Hewlett-Packard Company macht keine Angaben zur Eignung dieser Software für bestimmte Zwecke. Sie wird ohne Modifikationen und ohne Gewährleistung bereitgestellt.

Dieses Programm enthält STL-Software (STL = Standard Template Library) von Silicon Graphics Computer Systems, Inc. Copyright (c) 1996 - 1999.

- Die Berechtigung zum Verwenden, Kopieren, Ändern, Verteilen und Verkaufen dieser Software sowie der zugehörigen Dokumentation für die gewünschten Zwecke wird hiermit gebührenfrei erteilt. Voraussetzung hierfür ist allerdings, daß der o. a. Copyrightvermerk auf allen Kopien erscheint, und daß sowohl dieser Copyrightvermerk als auch dieser Berechtigungshinweis in der zugehörigen Dokumentation aufgeführt werden. Silicon Graphics macht keine Angaben zur Eignung dieser Software für bestimmte Zwecke. Sie wird ohne Modifikationen und ohne Gewährleistung bereitgestellt.

Andere Namen von Unternehmen, Produkten oder Dienstleistungen können Marken oder Dienstleistungsmarken anderer Unternehmen sein.

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden. Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, daß nur Programme, Produkte oder Dienstleistungen von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Dienstleistungen können auch andere ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb der Produkte, Programme und Dienstleistungen in Verbindung mit Fremdprodukten liegt beim Kunden, soweit solche Verbindungen nicht ausdrücklich von IBM bestätigt sind.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an IBM Europe, Director of Licensing, 92066 Paris La Defense Cedex, France, zu richten. Anfragen an obige Adresse müssen auf englisch formuliert werden.

Inhaltsverzeichnis

Vorwort ix

Zielgruppe ix

Referenzinformationen ix

Inhalt des Handbuchs x

In diesem Handbuch verwendete Konventionen xi

Kontaktaufnahme zur Kundenunterstützung xi

Tivoli PKI - Webinformationen xi

Kapitel 1. Informationen zu Tivoli PKI 1

Kapitel 2. Übersicht 3

Kapitel 3. Informationen zur Vorgehensweise 5

Registrierung als Registrator 5

Aktivieren eines Browsers 6

Zugreifen auf die Webseite für die Registrierung 6

Anfordern eines Browserzertifikats 7

Prüfen des Registrierungsstatus 9

Abrufen von Berechtigungen 10

Installieren von RA Desktop 10

Rekonfigurieren von RA Desktop 11

Zugreifen auf RA Desktop 12

Arbeiten mit Abfragen 12

Übergeben einer Abfrage 12

Abrufen von anstehenden Zertifikatsanforderungen 13

Abrufen von anstehenden Schlüsselwiederherstellungsanforderungen 13

Abrufen von ablaufenden Zertifikaten 14

Auswählen eines Datums aus dem Kalender 14

Definieren eines Grenzwerts für die Anzahl von abzurufenden Datensätzen 15

Definieren der Anzahl von Sätzen pro Seite 15

Abrufen von Rückmeldungen während der Verarbeitung 15

Arbeiten mit Ergebnissen 15

Anzeigen von Abfrageergebnissen 15

Anzeigen von Ergebnissen auf mehreren Seiten 17

Anzeigen von Details eines Elements 17

Anzeigen der Attribute von Elementen 17

Anzeigen von Aktionsprotokollen 18

Wechseln zwischen Registerkarten 19

Anpassen der Größe von Tabellenspalten 19
Sortieren von Tabellenzeilen nach bestimmten Spalten 20
Auswählen von Datensätzen in Tabellen. 20
Ausführen von Aktionen 20
Ausführen von Aktionen für mehrere Datensätze 20
Ausführen von Aktionen für einzelne Datensätze 21
Ändern eines Attributwerts 22
Ändern eines Gültigkeitszeitraums 22
Angeben des Anforderungsprofils 23
Hinzufügen eines Kommentars. 23
Genehmigen einer Anforderung 24
Genehmigen einer Schlüsselwiederherstellungsanforderung. 24
Behalten einer Anforderung im Status ″anstehend″ 24
Zurückweisen einer Anforderung 24
Zurückweisen einer Schlüsselwiederherstellungsanforderung. 25
Ändern der Erneuerbarkeit. 25
Aussetzen eines Zertifikats 25
Widerrufen eines Zertifikats. 26
Wiederaufnehmen eines Zertifikats. 26
Publizieren eines Zertifikats. 27
Prüfen der Berechtigungen für die Domäne 27
Beenden von RA Desktop 27
Deinstallieren von RA Desktop 28

Kapitel 4. Erläuterungen 29

Registrierung. 29
Vorabregistrierung 29
Webbrowserunterstützung 30
Registrierung. 30
Unternehmensregel 30
Registrierungsstellen 31
Registrierungsdatenbanken. 31
Registrierungsdomänen 31
Registrierungssätze 32
Datensatzattribute 32
Zertifizierung 32
Zertifikatsaussteller 32
Zertifikatswiderrufslisten (CRL). 32
Verzeichnisse (Directory). 33

Registrierte Namen 33
Zertifikate 33
Browserzertifikate 33
CA-Zertifikate 34
Server- oder Einheitenzertifikate 34
Zertifikatserweiterungen 34
Gültigkeitsdauer von Zertifikaten 34
Aussetzen und Wiederaufnehmen von Zertifikaten 35
Erneuerbarkeit 35
Sicherung und Wiederherstellung von Zertifikatsschlüsseln 35
Publizieren von Zertifikaten 36
Verwaltung 36
Zugriffssteuerung 36
Authentifizierung und Berechtigung 36
Parallele Verwaltung 36
Servlet zur Unterstützung von RA Desktop 36
Anforderungsprofile 37

Kapitel 5. Referenzinformationen 39

Registerkarte 'Abfrage' 39
Abfragefelder 39
Vordefinierte Abfragen 43
Anzahl der abzurufenden Datensätze - Optionen 44
Sätze pro Seite - Optionen 44
Registerkarte 'Ergebnisse' 44
Verwaltungsaktionen 45
Gründe für das Widerrufen eines Zertifikats 46
Registerkarte 'Details' 46
Aktionsprotokoll - Ereignisse 47
Attribute von Anforderungen und Zertifikaten 47
Zertifikatserweiterungen 49
Gelieferte Zertifikatstypen 49
Detailgruppen 50
Status der Registrierungsanforderungen 51
Hilfe für Registerkarten 52
JVM für Internet Explorer 52
Tastaturalternativen zur Bedienung mit der Maus 53
Fehlerbehebung 56

Glossar **57**

Index **77**

Vorwort

Dieses Handbuch enthält Informationen darüber, wie die Registrierungsaktivitäten für Tivoli PKI-Zertifikate mit Hilfe von Registration Authority (RA) Desktop verwaltet werden.

Dieses Release des Produkts unterstützt lediglich AIX-Plattformen. Alle Materialien, die sich mit Microsoft Windows befassen, sollten ignoriert werden.

Zielgruppe

Dieses Handbuch stellt Administratoren Task-orientierte Informationen zur Verwaltung von Tivoli PKI-Zertifikaten während ihrer Gültigkeitsdauer zur Verfügung.

Benutzer dieses Handbuchs sollten über praktische Erfahrung in der Ausführung von Datenbankabfragen und der Tätigkeit eines Registrators verfügen und sich mit webbasierten Anwendungen auskennen.

Referenzinformationen

Die Tivoli PKI-Produktdokumentation steht im PDF- (Portable Document Format) sowie im HTML-Format auf der Tivoli-Website zur Verfügung. HTML-Versionen bestimmter Veröffentlichungen werden zusammen mit dem Produkt installiert und können über die Benutzerschnittstelle aufgerufen werden.

Hierbei ist zu beachten, dass am Produkt selbst seit der Erstellung der Veröffentlichungen möglicherweise Änderungen vorgenommen wurden. Die neuesten Produktinformationen sowie Informationen für den Zugriff auf Veröffentlichungen in den von Ihnen gewünschten Sprachen und Formaten enthalten die Release-Informationen. Die neueste Version der Release-Informationen steht auf der Tivoli Public Key Infrastructure-Website zur Verfügung:

`http://www.tivoli.com/support`

Die Tivoli PKI-Bibliothek umfasst die folgenden Dokumentationen:

Einführung
: Dieses Handbuch bietet einen Überblick über das Produkt. Es enthält eine Aufstellung der Produktvoraussetzungen, Erläuterungen zu den Installationsverfahren und Informationen über den Zugriff auf die Online-Hilfefunktion für alle Produktkomponenten. Es liegt in gedruckter Form vor und wird zusammen mit dem Produkt ausgeliefert.

Systemverwaltung
: Dieses Handbuch enthält Basisinformationen zur Verwaltung eines Tivoli PKI-Systems. Außerdem werden in diesem Handbuch die Prozeduren zum Starten und Stoppen der Server, Ändern der Kennwörter, Verwalten der Serverkomponenten, Durchführen von Prüfungen sowie zum Ausführen von Datenintegritätsprüfungen erläutert.

Konfiguration
: Dieses Handbuch enthält Informationen zur Verwendung des Setup Wizards zum Konfigurieren eines Tivoli PKI-Systems. Sie können auf die HTML-Version dieses Handbuchs zugreifen, während Sie die Onlinehilfefunktion für den Assistenten anzeigen.

RA Desktop

Dieses Handbuch enthält Informationen zur Verwendung von RA Desktop für die Verwaltung von Zertifikaten während ihres Gültigkeitszeitraums. Sie können auf die HTML-Version dieses Handbuchs zugreifen, während Sie die Onlinehilfefunktion für den Desktop anzeigen.

Benutzerhandbuch

Dieses Handbuch enthält Informationen zum Abrufen und Verwalten von Zertifikaten. Es stellt Prozeduren zum Verwenden der Browserregistrierungsformulare von Tivoli PKI für die Anforderung, Erneuerung und den Widerruf von Zertifikaten bereit. Außerdem enthält es eine Erläuterung zur Vorabregistrierung bei PKIX-kompatiblen Zertifikaten.

Anpassung

Dieses Buch enthält Informationen dazu, wie Sie die Tivoli PKI-Registrierungsfunktion für die Unterstützung der Registrierungs- und Zertifizierungsziele Ihrer Unternehmensregeln anpassen können. So erhalten Sie beispielsweise Anweisungen zur Anpassung von HTML- und Java-Serverseiten, Benachrichtigungsschreiben, Zertifikatsprofilen und Regel-Exits.

Inhalt des Handbuchs

Dieses Handbuch enthält folgende Informationen:

- „Informationen zu Tivoli PKI” auf Seite 1 liefert eine kurze Beschreibung der Funktionen und des Leistungsspektrums von Tivoli PKI.
- „Übersicht” auf Seite 3 beschreibt den Aufgabenbereich des Administrators bzw. Registrators sowie einige typische Tasks, die mit Hilfe von RA Desktop ausgeführt werden.
- „Informationen zur Vorgehensweise” auf Seite 5 enthält Task-orientierte Informationen und Anleitungen zur Ausführung der Aufgaben eines Registrators.
- „Erläuterungen” auf Seite 29 enthält Beschreibungen zu den Konzepten, die sich auf die Registrierung, Zertifizierung und Verwaltung unter RA Desktop beziehen.
- „Referenzinformationen” auf Seite 39 enthält Feldbeschreibungen, gültige Feldwerte und die Bedeutung von Attributen, die in RA Desktop angezeigt werden.
- „Glossar” auf Seite 57 definiert die Termini und Abkürzungen, die in diesem Handbuch verwendet werden und die möglicherweise neu oder unbekannt sind, sowie Termini, die von Bedeutung sein könnten.

In diesem Handbuch verwendete Konventionen

In diesem Handbuch werden für bestimmte Termini und Aktionen verschiedene Konventionen hinsichtlich des Schriftbilds verwendet. Die Schriftbilder haben folgende Bedeutung:

Schriftbild	Bedeutung
Fettdruck	Befehle, Schlüsselwörter, Markierungen und andere Informationen, die im genauen Wortlaut verwendet werden müssen, werden **fett** gedruckt.
Kursivdruck	Variablen, die angegeben werden müssen, sowie neue Termini werden *kursiv* gedruckt. Hervorgehobene Wörter und Ausdrücke werden ebenfalls *kursiv* gedruckt.
Monospace-Schrift	Codebeispiele, Ausgabe und Systemnachrichten werden in einer `Monospace-Schrift` gedruckt.

Kontaktaufnahme zur Kundenunterstützung

Wenn mit irgendeinem Tivoli-Produkt Probleme auftreten, können Sie über **http://www.support.tivoli.com** die Homepage der Tivoli-Unterstützung (Tivoli Support) aufrufen. Nachdem Sie eine Verbindung zum Kundenregistrierungsformular hergestellt und dieses übergeben haben, können Sie auf eine Reihe von Kundenunterstützungsservices auf dem Web zugreifen.

Kunden in Deutschland, Österreich oder der Schweiz können eine der folgenden Telefonnummern anrufen:

- Deutschland: **01805-00-1242**
- Österreich: **01-1706-6000**
- Schweiz: **0800-555454**

Ihre Meinung zu Tivoli-Produkten und der Tivoli-Dokumentation interessiert uns. Gerne nehmen wir Verbesserungsvorschläge Ihrerseits entgegen. Falls Sie Kommentare oder Anregungen zur vorliegenden Dokumentation haben, senden Sie uns bitten eine E-Mail an folgende Adresse: pubs@tivoli.com.

Tivoli PKI - Webinformationen

Kunden von Tivoli und IBM Tivoli finden Onlineinformationen zu allen Tivoli-Sicherheitsprodukten und Tivoli PKI.

Um wichtige Informationen über kurzfristigen Produktaktualisierungen oder Serviceinformationen zu Tivoli PKI abzurufen, beginnen Sie auf folgender Website: **http://www.tivoli.com/support/secure_download_bridge.html**

Informationen zum Produkt Tivoli Public Key Infrastructure erhalten Sie auf folgender Website: **http://www.tivoli.com/products/index/secureway_public_key/**

Informationen zu anderen Sicherheitsverwaltungsprodukten von Tivoli erhalten Sie unter folgender Webadresse: **http://www.tivoli.com/products/solutions/security/**

1

Informationen zu Tivoli PKI

Mit Tivoli Public Key Infrastructure (Tivoli PKI) sind Anwendungen in der Lage, Benutzer zu authentifizieren und eine gesicherte Kommunikation zu gewährleisten. Das Leistungsspektrum umfasst Folgendes:

- Ausstellung, Veröffentlichung und Verwaltung digitaler Zertifikate in Übereinstimmung mit den jeweiligen Registrierungs- und Zertifizierungsregeln eines Unternehmens.
- Unterstützung für die Verschlüsselungsstandards Public Key Infrastructure für X.509 Version 3 (PKIX) und Common Data Security Architecture (CDSA) zur Realisierung der Interoperabilität zwischen verschiedenen Lieferanten und Herstellern.
- Digitale Unterzeichnung und gesicherte Protokolle zur Authentifizierung aller an einer Transaktion beteiligten Parteien.
- Optimale Flexibilität durch browser-basierte Registrierungsfunktionen.
- Unterstützung zur Gewährleistung der Vertraulichkeit durch verschlüsselte Kommunikation und gesicherte Speicherung der Registrierungsinformationen.

Ein Tivoli PKI-System kann auf Serverplattformen unter IBM AIX/6000 und Microsoft Windows NT ausgeführt werden. Es umfasst die folgenden Hauptmerkmale:

- Ein zuverlässiger Zertifikatsaussteller (CA) verwaltet die Gültigkeitsdauer digitaler Zertifikate. Um die Authentizität eines Zertifikats zu belegen, unterzeichnet der CA jedes ausgestellte Zertifikat digital. Außerdem unterzeichnet der CA Zertifikatswiderrufslisten (CRLs), um zu bestätigen, dass ein bestimmtes Zertifikat nicht mehr gültig ist. Um seinen Signierschlüssel zusätzlich zu schützen, können Sie Verschlüsselungshardware (wird auch als Hardwaresicherheitsmodul, HSM bezeichnet) verwenden, z. B. den IBM SecureWay 4758 PCI Cryptographic Coprocessor.
- Eine Registrierungsstelle (RA) führt die Verwaltungsaufgaben aus, die bei der Benutzerregistrierung notwendig sind. Die RA stellt sicher, dass nur solche Zertifikate ausgestellt werden, die Ihre Unternehmensaktivitäten unterstützen, und dass diese Zertifikate nur an berechtigte Benutzer ausgegeben werden. Die Verwaltungsaufgaben können über automatisierte Prozesse oder auf der Basis menschlicher Entscheidungen ausgeführt werden.

  Ähnlich wie der CA können Sie zum Schutz des Signierschlüssels auch IBM SecureWay 4758 PCI Cryptographic Coprocessor verwenden.
- Eine Web-Schnittstelle für die Registrierung vereinfacht das Abrufen von Zertifikaten für Browser, Server und andere Einheiten und Zwecke, z. B. VPN-Einheiten (VPN = Virtual Private Network), Smart Cards und die sichere Übertragung von E-Mails.

- Eine Web-Verwaltungsschnittstelle, das RA Desktop, ermöglicht berechtigten Registratoren das Genehmigen oder Zurückweisen von Registrierungsanforderungen sowie das Verwalten von Zertifikaten nach deren Ausstellung.
- Ein Prüfsubsystem berechnet einen Nachrichtenauthentifizierungscode (Message Authentication Code, MAC) für jeden Protokolleintrag. Wenn Prüfdaten nach ihrer Aufzeichnung in der Prüfdatenbank geändert oder gelöscht werden, können Sie mit Hilfe des MAC diese Manipulation feststellen.
- Regel-Exits und Geschäftsprozessobjekte (Business Process Objects, BPO) ermöglichen Anwendungsentwicklern die Anpassung der Registrierungsprozesse.
- Integrierte Unterstützung für eine Verschlüsselungsmaschine. Zur Authentifizierung der Kommunikation werden die Tivoli PKI-Hauptkomponenten mit einem werkseitig generierten privaten Schlüssel unterzeichnet. Sicherheitsobjekte, z. B. Schlüssel und MACs, werden verschlüsselt und in geschützten Bereichen (so genannten KeyStores oder Schlüsselspeichern) gespeichert.
- Integrierte Unterstützung für IBM Directory. Das Directory speichert Informationen zu gültigen und widerrufenen Zertifikaten in einem LDAP-kompatiblen Format.
- Integrierte Unterstützung für IBM WebSphere Application Server und IBM HTTP Server. Der Webserver arbeitet mit dem RA-Server, um Nachrichten zu verschlüsseln, Anforderungen zu authentifizieren und Zertifikate an den gewünschten Empfänger zu übertragen.
- Integrierte Unterstützung für IBM DB2 Universal Database.

2

Übersicht

Wenn ein Unternehmen mit sicheren Anwendungen arbeitet, die durch Tivoli PKI geschützt werden, können nur Benutzer mit den richtigen Identitätsnachweisen auf diese Anwendungen zugreifen. Ein Benutzer, der einen solchen Identitätsnachweis (z. B. ein digitales Zertifikat) benötigt, kann es anfordern, indem er der für die Ausstellung zuständigen Stelle die entsprechenden Informationen zur Verfügung stellt. Die Daten in der Registrierungsanforderung bilden die Basis, auf der über die Genehmigung oder Zurückweisung der Anforderung entschieden wird. Wenn eine Registrierungsanforderung genehmigt wird, verarbeitet die Registrierungsstelle (RA) von Tivoli PKI die Anforderung und der Zertifikatsaussteller (CA) von Tivoli PKI stellt das Zertifikat aus. Die Datensätze, die für die Registrierungsanforderungen und Zertifikate aufgezeichnet wurden, werden in einer verschlüsselten Registrierungsdatenbank gespeichert.

Die Auswertung von Registrierungsanforderungen und die Verwaltung dieser Datensätze sind Verwaltungsaufgaben. In manchen Unternehmen ist Tivoli PKI so konfiguriert, dass Teile dieser Aufgaben automatisch ausgeführt und die Registrierungsdaten durch ein Programm ausgewertet werden. In anderen Fällen werden die bei der Registrierung notwendigen Entscheidungen von einem Registrator getroffen.

Bei Tivoli PKI Registration Authority Desktop (RA Desktop) handelt es sich um eine grafische Benutzerschnittstelle (GUI) zur Bearbeitung von Registrierungsanforderungen und zur Verwaltung der hierbei generierten Datensätze. Es dient zur Unterstützung des Registrators bei folgenden Aufgaben:

- Auswerten der anstehenden Registrierungsanforderungen, um diese zu genehmigen oder zurückzuweisen.
- Vorbereiten der Abfragen zum Abrufen von Datensätzen für Zertifikate eines bestimmten Typs oder für einen bestimmten Benutzer.
- Prüfen der Details eines Datensatzes.
- Definieren des Gültigkeitszeitraums eines Zertifikates.
- Ausführen von Aktionen zum Ändern des Status eines Zertifikates oder einer Registrierungsanforderung.
- Kommentieren eines Datensatzes zur Erläuterung des Grundes für eine ausgeführte Aktion.
- Genehmigung von Wiederherstellungsanforderungen für private Zertifikatsschlüssel aus gesicherten PKCS #12-Dateien.

Bei RA Desktop handelt es sich um ein sicheres Applet. Zu seiner Verwendung müssen Sie über die Berechtigung zur Ausführung bestimmter Aufgaben verfügen und sich durch Vorlage des korrekten digitalen Zertifikats authentifizieren.

Zugehörige Abschnitte:

„Registrierung als Registrator” auf Seite 5
„Zugreifen auf RA Desktop” auf Seite 12

3

Informationen zur Vorgehensweise

Die Abschnitte in diesem Kapitel enthalten Anweisungen zur Ausführung der folgenden Aufgaben eines Registrators:

- Vorbereiten des Browsers und Installieren von RA Desktop
- Abrufen des Browser-Zertifikats und der Berechtigung als Registrator
- Abfragen der Registrierungsdatenbank zum Arbeiten mit Anforderungen und Zertifikaten

Registrierung als Registrator

Bevor Sie auf RA Desktop zugreifen können, um Zertifikate und Zertifikatsanforderungen zu verwalten, müssen Sie eine Registrierung als berechtigter Tivoli PKI-Registrator durchführen. Dieser Prozess umfasst mehrere Schritte, von denen einige durch einen Systemadministrator ausgeführt werden müssen.

Dieser Abschnitt beschreibt die vorbereitenden Aufgaben, die vor der Verwendung von RA Desktop ausgeführt werden müssen:

__ Schritt 1. Ein Benutzer, normalerweise ein Systemadministrator, muss die Prozeduren im Handbuch *Systemverwaltung* ausführen, um den ersten Registrator zum System hinzuzufügen.

__ Schritt 2. Konfigurieren des Web-Browsers für die Ausführung von RA Desktop.

__ Schritt 3. Zugreifen auf die Tivoli PKI-Web-Seite für die Registrierung, um die erforderliche Zertifizierung abzurufen.

__ Schritt 4. Anfordern eines CA-Zertifikats und anschließend eines Browser-Zertifikats für den verwendeten Web-Browser. Richtlinien zum Typ des Browser-Zertifikats, das Sie für die Installation auswählen müssen, sowie zum Namen der Registrierungsdomäne, für deren Verwaltung Sie berechtigt werden, erhalten Sie beim jeweiligen Unternehmen.

__ Schritt 5. Überprüfen des Registrierungsstatus und Sicherstellen, dass das Zertifikat installiert wurde.

__ Schritt 6. Nach der Ausstellung des Zertifikats müssen Sie die Berechtigung zur Ausführung von Registratoraufgaben anfordern. Senden Sie eine Anforderung an den ersten berechtigten Registrator und stellen Sie diesem Benutzer die Anforderungs-ID zur Verfügung, die Sie nach der Übergabe Ihrer Zertifikatsanforderung erhalten haben.

__ Schritt 7. Der erste Registrator muss die im Handbuch *Systemverwaltung* beschriebenen Prozeduren ausführen, um Sie als neuen Registrator zu berechtigen.

__ Schritt 8. Installieren von RA Desktop, nachdem Sie die Bestätigung erhalten haben, dass Sie als Registrator registriert wurden.

Wenn Sie den während der Installation definierten Standardbrowser zu einem späteren Zeitpunkt ändern möchten oder wenn eine Änderung der Webadresse für den RA-Server erforderlich ist, können Sie eine Rekonfiguration von RA Desktop durchführen.

Aktivieren eines Browsers

Vor dem Aktivieren eines Browsers muss sichergestellt werden, dass die verwendete Maschine die nachfolgend aufgeführten Anforderungen für die Ausführung von RA Desktop erfüllt:

- Intel Pentium-Prozessor mit mindestens 64 MB RAM
- Computerbildschirm, der VGA-Auflösung oder höhere Auflösungen unterstützt
- Betriebssystem Microsoft Windows 95, 98 oder NT

Gehen Sie wie folgt vor, um einen Web-Browser für RA Desktop zu aktivieren:

1. Installieren Sie einen der unterstützten Web-Browser:
   - Netscape Navigator oder Netscape Communicator, nur Release 4.7 *x*
   - Microsoft Internet Explorer, ab Release 5.0

     Als Voraussetzung für Internet Explorer müssen Sie JVM (Java Virtual Machine) ab Release 5.00, Build 3167 installieren. Im Abschnitt „JVM für Internet Explorer" auf Seite 52 wird beschrieben, wie Sie das aktuelle JVM-Release feststellen und bei Bedarf eine Erweiterung vornehmen können.

   Anmerkung: Sie müssen die offizielle Version des Produkts installieren, die über Netscape oder Microsoft bezogen werden kann. Mit Versionen anderer Anbieter können möglicherweise bestimmte Informationen nicht korrekt angezeigt werden. Dies gilt besonders dann, wenn das Applet in einer anderen Sprache als Englisch ausgeführt wird.
2. Nehmen Sie die erforderlichen Änderungen bei Ihrem Web-Browser vor:
   - Öffnen Sie hierzu in Netscape das Menü **Einstellungen**, um Java zu aktivieren.
   - Öffnen Sie hierzu im Internet Explorer das Menü **Optionen**, um Java zu aktivieren.

Anmerkung: Die neuesten Informationen zu den RA Desktop-Applet-Anforderungen finden Sie in den Release-Informationen. Die Release-Informationen stehen auf der Tivoli Public Key Infrastructure-Website zur Verfügung:

`http://www.tivoli.com/support`

Zugreifen auf die Webseite für die Registrierung

Gehen Sie wie folgt vor, um auf die Web-Seite für die Registrierung zuzugreifen:

1. Rufen Sie die in Ihrem Unternehmen verwendete Webadresse für den Zugriff auf die Webseite für die Registrierung ab. Die Webadresse weist das folgende Format auf:

   http://MyWebServer:port/MyDomain/index.jsp

   Dabei stellt *MyWebServer:port* den Host-Namen und den Anschluss des Servers dar, auf dem die Tivoli PKI-Registrierungsstelle installiert ist. *MyDomain* gibt den konfigurierten Namen der Registrierungsdomäne auf dem aktuellen Tivoli PKI-System an. Beispiel:

```
http://MyWebServer:80/MyDomain/index.jsp
```

2. Öffnen Sie den Browser, der für RA Desktop aktiviert wurde.
3. Geben Sie die Webadresse ein:
   - Geben Sie in Netscape die Webadresse im Textfenster bei **Adresse** ein.
   - Geben Sie im Internet Explorer die Webadresse im Textfenster bei **Adresse** ein.
4. Drücken Sie anschließend die **Eingabetaste**.

   Daraufhin wird die Tivoli PKI-Web-Seite für die Registrierung angezeigt. Bei einer Standardinstallation lautet der Name dieser Seite ″Identitätsnachweis - Verwaltung″ (Credential Central).
5. Wenn Sie die Tivoli PKI-Registrierungsservices zum ersten mal verwenden, klicken Sie auf die Option **CA-Zertifikat für den jeweiligen Server in Ihrem Browser installieren**.

   Dieses Zertifikat ermöglicht dem verwendeten Browser die Authentifizierung der Kommunikation mit den Registrierungsservices. Wenn Sie diese Services das nächste Mal verwenden, müssen Sie diesen Schritt nicht mehr ausführen.

Anfordern eines Browserzertifikats

Dieser Abschnitt beschreibt die Verwendung der Tivoli PKI-Seite für die Registrierung zum Anfordern eines Browser-Zertifikats. Dieses Zertifikat wird zur Ausführung von RA Desktop benötigt.

Anmerkung: Als Registrator müssen Sie möglicherweise auch Server oder andere Einheiten registrieren oder für bestimmte Benutzer eine Vorabregistrierung durchführen. Weitere Informationen zur Ausführung dieser Aufgaben enthält das *Tivoli PKI Benutzerhandbuch*.

Abhängig von der Anpassung der Registrierungsfunktion in Ihrem Unternehmen können die Prozeduren, die zum Abrufen eines gültigen Zertifikats ausgeführt werden müssen, variieren. Die folgenden Erläuterungen geben einen allgemeinen Überblick zu den grundlegenden Arbeitsschritten. Wenn Sie Informationen zu den unternehmensspezifischen Prozeduren in Ihrer Systemumgebung benötigen, wenden Sie sich bitte an den zuständigen Systemadministrator.

Gehen Sie wie folgt vor, um ein Browser-Zertifikat abzurufen:

1. Führen Sie mit Ihrem Browser einen Zugriff auf die Registrierungs-Web-Seite aus.
2. Führen Sie unter **Zertifikatsregistrierung** folgende Schritte aus:
   a. Wählen Sie **Registrierungstyp → Browser-Zertifikat** aus.
   b. Wählen Sie **Aktion → Registrieren** aus.
   c. Klicken Sie auf **OK**. Daraufhin wird das angeforderte Registrierungsformular angezeigt.
3. Befolgen Sie die Anweisungen auf der Web-Seite zum Ausfüllen der Felder. Es gibt zwei Abschnitte:
   - Im Abschnitt **Registrierungsinformationen** befinden sich Textfenster, in die Sie persönliche Daten eintragen.

- Der Abschnitt **Zertifikatsanforderungsinformationen** enthält Textfenster, in denen Daten zum gewünschten Zertifikat angegeben werden müssen. Wenn Sie in den wahlfreien Feldern des Abschnitts keine Werte eingeben, werden die von Tivoli PKI bereitgestellten Standardwerte verwendet, die sich nach dem angeforderten Zertifikatstyp richten.

Hierbei sind die folgenden Felder besonders zu beachten:

Zertifikatstyp
Wählen Sie den Browser-Zertifikatstyp aus, dessen Vorlage Ihr Unternehmen für den Zugriff auf RA Desktop anfordert. Unter „Gelieferte Zertifikatstypen" auf Seite 49 werden die verschiedenen Zertifikatstypen beschrieben.

Das CA-Zertifikat auf dem Browser installieren
Klicken Sie auf diesen Knopf, um ein CA-Zertifikat abzurufen, das mit dem Zertifikatstyp kompatibel ist. Wenn Sie auf diesen Knopf klicken, wird das CA-Zertifikat sofort heruntergeladen.

Dieses Zertifikat ermöglicht dem Browser die Authentifizierung der Kommunikation mit der Registrierungsfunktion, wenn Sie RA Desktop verwenden. Wenn Sie aus einem bestimmten Grund bereits über ein identisches CA-Zertifikat verfügen, wird kein weiteres Zertifikat desselben Typs benötigt.

E-Mail-Adresse
Um das Feld **E-Mail-Benachrichtigung** auszuwählen, müssen Sie Ihre E-Mail-Adresse angeben.

E-Mail-Benachrichtigung
Wählen Sie dieses Feld aus, um eine E-Mail mit dem Ergebnis Ihrer Anforderung zu erhalten.

Anmerkung: Wenn der RA-Server in Ihrem Unternehmen auf einer Windows NT-Plattform installiert ist, muss die Konfigurationsdatei (raconfig.cfg) der Registrierungsfunktion möglicherweise so aktualisiert werden, dass sie einen Verweis auf einen SMTP-Host enthält, um diese Funktion zu aktivieren. Einzelheiten hierzu finden Sie im Handbuch *Tivoli PKI Anpassung*.

Identifikationsprüfungsantwort
Vergessen Sie nicht die angegebene **Identifikationsprüfungsantwort**, bei der die Groß-/Kleinschreibung beachtet werden muss. Sie benötigen diese später, um den Status der Registrierungsanforderung zu prüfen.

Domänenname
Wahlweise kann der Host-Name der Maschine angegeben werden, auf der das Zertifikat installiert werden soll (der Host-Name Ihrer Maschine). Normalerweise muss in diesem Feld keine Angabe gemacht werden, es sei denn, die Verwendung des Felds wurde explizit angefordert.

Zusätzliche Unterstützung zu diesen Feldern finden Sie im Abschnitt mit Referenzinformationen im *Tivoli PKI Benutzerhandbuch*.

4. Klicken Sie auf **Registrierungsanforderung übergeben**.

   Nach dem Empfang des Registrierungsformulars durch Tivoli PKI werden diese Informationen vom Programm geprüft:

- Wenn das Formular Fehler enthält, werden diese angezeigt. Führen Sie die erforderlichen Änderungen durch und klicken Sie anschließend auf **Registrierungsanforderung erneut übergeben**.
- Wenn das Formular keine Fehler enthält, wird auf einer weiteren Web-Seite Ihre Anforderungs-ID angezeigt.

5. Diese sollte unbedingt aufbewahrt werden. Sie dient später zu Ihrer Identifikation, wenn Sie den Status der Anforderung prüfen und Ihr Zertifikat empfangen möchten, nachdem es ausgestellt ist. Führen Sie einen der auf der Web-Seite beschriebenen Arbeitsschritte aus:
   - Setzen Sie auf dieser Web-Seite ein Lesezeichen, so dass Sie diese Anzeige erneut aufrufen und Ihr Zertifikat überprüfen können. Dies ist die einfachste Möglichkeit, den Status zu einem späteren Zeitpunkt zu überprüfen.
   - Notieren Sie die Anforderungs-ID, um diese ggf. angeben zu können. Als zusätzliche Sicherheitsmaßnahme empfiehlt es sich, die Anforderungs-ID in jedem Fall zu notieren, unabhängig davon, ob Sie für die Statusseite ein Lesezeichen gesetzt haben.
   - Wenn Sie bei der Registrierung im entsprechenden Feld angegeben haben, dass Sie eine E-Mail-Benachrichtigung wünschen, erhalten Sie die Anforderungs-ID per E-Mail.

Prüfen des Registrierungsstatus

Um den Status Ihrer Registrierungsanforderung zu prüfen, müssen Sie entweder auf die Web-Seite zurückkehren, auf der Sie während der Registrierung ein Lesezeichen gesetzt haben, oder die folgenden Arbeitsschritte ausführen:

1. Führen Sie einen Zugriff auf die Registrierungs-Web-Seite aus.
2. Wählen Sie unter **Registrierungstyp** den Typ der angeforderten Registrierung aus.
3. Wählen Sie unter **Aktion** die Option **Registrierungsstatus überprüfen** aus.
4. Klicken Sie auf **OK**.

   Die Anzeige enthält Felder, in denen Sie eine Authentifizierung durchführen müssen, bevor Sie Informationen zu Ihrer Anforderung abrufen können.
5. Gehen Sie wie folgt vor, um in den Feldern Informationen anzugeben:
   - Geben Sie unter **Anforderungs-ID** die Anforderungs-ID ein, die nach der Übergabe des Registrierungsformulars angezeigt wurde.
   - Geben Sie unter **Identitätsprüfungsantwort** denselben Wert ein wie auf dem Registrierungsformular.
6. Klicken Sie auf **Registrierungsstatus überprüfen**.

   Daraufhin wird eine Nachricht mit dem aktuellen Status Ihrer Anforderung angezeigt:
   - Wenn Ihre Anforderung weiterhin ansteht, können Sie den Status zu einem späteren Zeitpunkt nochmals prüfen.
   - Wurde Ihr Browser-Zertifikat bereits ausgestellt, wird es heruntergeladen, wenn Sie auf **Registrierungsstatus überprüfen** klicken.
7. Sie können das Zertifikat nun anzeigen. Befolgen Sie hierzu die auf der Web-Seite aufgeführten Anweisungen.

Abrufen von Berechtigungen

Bevor Sie den zuständigen Systemadministrator bitten, Sie für RA Desktop zu berechtigen, sollten Sie folgende Arbeitsschritte ausführen:

- Fordern Sie ein Browser-Zertifikat an und geben Sie hierbei die Registrierungsdomäne ein, die Sie verwalten werden.
- Laden Sie das Browser-Zertifikat sowie das kompatible CA-Zertifikat auf Ihren Web-Browser herunter.

Installieren von RA Desktop

Die Installation von RA Desktop ist ein Prozess, der aus zwei Teilen besteht. Bei der Installation der Server-Software muss ein Systemadministrator **RA Desktop** auswählen, um das Installationsabbild für das Applet zu installieren. Anschließend muss der Administrator das Abbild verteilen oder im Netz zur Verfügung stellen, so dass das Installationsprogramm von den einzelnen Workstations aus ausgeführt werden kann.

Anmerkung: Wenn Sie das RA Desktop-Applet auf derselben Maschine installieren, auf der zuvor der Setup Wizard ausgeführt wurde, kann der Setup Wizard auf dieser Maschine nicht erneut ausgeführt werden. Wenn Sie Tivoli PKI in einer Testumgebung verwenden, empfiehlt es sich, den Setup Wizard und RA Desktop auf verschiedenen Maschinen zu installieren. Auf diese Weise können Sie den Konfigurationsprozess so lange wiederholen, bis das System in den Produktionsmodus gesetzt werden kann.

Führen Sie die folgende Prozedur aus, um das RA Desktop-Installationsprogramm RADInst.exe auszuführen.

1. Stellen Sie sicher, dass die verwendete Workstation die im Abschnitt „Aktivieren eines Browsers” auf Seite 6 aufgeführten Anforderungen erfüllt.
2. Fordern Sie bei Ihrem Systemadministrator die Webadresse für die Registrierungsdomäne an, die Sie verwalten werden.
3. Gehen Sie den Anweisungen Ihres Unternehmens entsprechend vor, um das RA Desktop-Installationsabbild zu kopieren, herunterzuladen bzw. darauf zuzugreifen.
4. Beenden Sie alle aktiven Programme.
5. Wählen Sie **Start → Ausführen** aus, klicken Sie auf **Durchsuchen**, um nach der Datei RADInst.exe zu suchen, und klicken Sie anschließend auf **OK**, um das Programm auszuführen.
6. Lesen Sie die Informationen im Eingangsfenster und klicken Sie anschließend auf **Weiter**.
7. Klicken Sie im Fenster ’Zielpfad wählen’ auf **Weiter**, wenn Sie die Software im Standardpfad (c:\Program Files\IBM\Trust Authority\RA Desktop) installieren möchten. Klicken Sie andernfalls auf **Durchsuchen**, um einen anderen Zielordner auszuwählen bzw. einzugeben. Klicken Sie anschließend auf **Weiter**.
8. Wählen Sie im Fenster ’Browser auswählen’ den Browser aus, der als Standardbrowser für den Zugriff auf RA Desktop verwendet werden soll.

   Anmerkung: Dieses Fenster wird nur dann angezeigt, wenn sowohl ein Microsoft- als auch ein Netscape-Browser installiert ist und beide den erforderlichen Releasestand aufweisen.

9. Geben Sie im Fenster 'Host auswählen' die Webadresse für den Server ein, auf dem die Registrierungsstelle (RA) installiert ist. Die URL muss im nachfolgend aufgeführten Format eingegeben werden. Dabei gilt: *hostname:port* stellt den virtuellen Host-Namen und die Nummer des sicheren Anschlusses auf dem Server dar, auf dem die Registrierungsstelle installiert wurde. *RegistrationDomainName* ist der Name, der für die Registrierungsdomäne Ihres Unternehmens konfiguriert wurde.

   ```
   https://hostname:port/RegistrationDomainName
   ```

   Beispiel: **https://MyRAserver:1443/MyDomain**

10. Klicken Sie im Fenster 'Programmordner auswählen' auf **Weiter**, wenn Sie den Standardprogrammordner (IBM SecureWay Trust Authority) verwenden möchten. Geben Sie andernfalls den Namen des zu verwendenden Ordners ein bzw. wählen Sie diesen aus und klicken Sie anschließend auf **Weiter**.
11. Überprüfen Sie im Fenster 'Kopiervorgang starten' die Einstellungen, die Sie für diese Installation von RA Desktop angegeben haben. Klicken Sie auf **Weiter**, um die Einstellungen zu bestätigen. Die Dateien werden vom Programm in den angegebenen Pfad kopiert.
12. Führen Sie im Fenster 'Setup abgeschlossen' folgende Schritte aus:
    - Wählen Sie das Markierungsfeld zum Anzeigen der Readme-Datei aus, wenn Sie die Tivoli PKI-*Readme*-Datei lesen möchten. Die *Readme*-Datei wird im ausgewählten Browser angezeigt, nachdem Sie auf **Beenden** geklickt haben.
    - Klicken Sie auf **Beenden**, um den Installationsprozess abzuschließen.

Nach Abschluss der Installation befinden sich **RA Desktop** und **RA Desktop-Konfiguration** im Menü **Start** unter **Programme → IBM SecureWay Trust Authority**.

Rekonfigurieren von RA Desktop

Nach der Installation von RA Desktop können Sie den Standardbrowser ändern, der für den Zugriff auf das Applet verwendet werden soll. Darüber hinaus kann die Webadresse des RA-Servers geändert werden, auf dem sich das Applet befindet. Führen Sie die folgende Prozedur aus, um diese Änderungen vorzunehmen:

1. Wählen Sie **Start → Programme → IBM SecureWay Trust Authority → RA Desktop-Konfiguration** aus.
2. Wählen Sie im Fenster 'Browser auswählen' den Browser aus, der für den Zugriff auf RA Desktop verwendet werden soll.
3. Geben Sie im Fenster 'Host auswählen' die Webadresse für den RA-Server ein, auf dem RA Desktop installiert ist. Sie müssen den Namen des sicheren Hosts, die Anschlussnummer sowie den Namen der Registrierungsdomäne, die Sie verwalten sollen, angeben (der Domänenname darf keine Leerzeichen enthalten). Beispiel:

   https://NewRAServer:1443/NewDomainName

4. Klicken Sie im Fenster 'Programmordner auswählen' auf **Weiter**, ohne Änderungen vorzunehmen.
5. Überprüfen Sie im Fenster 'Kopiervorgang starten' die Änderungen und klicken Sie anschließend auf **Weiter**.
6. Klicken Sie im Fenster 'Setup abgeschlossen' auf **Beenden**, um den Rekonfigurationsprozess abzuschließen.

Zugreifen auf RA Desktop

Vor dem Starten von RA Desktop müssen Sie immer die folgenden Arbeitsschritte ausführen:

1. Wenn sich Ihr Registratorzertifikat auf dem Netscape-Browser befindet, müssen alle momentan ausgeführten Netscape-Sitzungen geschlossen werden.
2. Wählen Sie unter Windows die Optionen **Start → Programme → IBM SecureWay Trust Authority → RA Desktop** aus.

   Wenn Sie die Webadresse von RA Desktop anfordern, wird von Ihrem Webbrowser und dem zugehörigen Server eine gesicherte Sitzung (mit Client-Authentifizierung) initialisiert. Bevor der Server den Inhalt dieser Webadresse zurückgeben kann, müssen Sie sich als gültiger Registrator authentifizieren. Der Browser fordert Sie zur Vorlage eines Zertifikates auf. Die Darstellung dieser Aufforderung kann abhängig vom verwendeten Browser variieren.
3. Legen Sie Ihr Registratorzertifikat vor.

   Anmerkung: Wenn Sie mit dem Internet Explorer arbeiten, übergibt der Browser automatisch das letzte Zertifikat, das beim Server während der Browser-Sitzung vorgelegt wurde. Sie werden nicht zur Eingabe einer Bestätigung aufgefordert. Wenn Sie ein anderes Zertifikat vorlegen möchten, müssen Sie den Browser beenden und anschließend erneut starten.

   Der Web-Browser lädt das RA Desktop-Applet herunter und initialisiert es:

   - Während des Herunterladens des Applets werden möglicherweise unten in der Browser-Anzeige verschiedene Nachrichten angezeigt. Das System kann z. B. eine Nachricht ausgeben, um anzuzeigen, dass der Browser Java initialisiert.
   - Während der Initialisierung wird ein Statusbalken angezeigt, der den Fortschritt des Prozesses darstellt. Wenn bei der Initialisierung ein Fehler auftritt, wird der Statusbalken angehalten und eine generische Warnung angezeigt.

Nach dem Abschluss der Initialisierung wird RA Desktop angezeigt. Sie können es nun sofort einsetzen und mit der Verwaltung von Registrierungsanforderungen und Zertifikaten für die Registrierungsdomäne beginnen, die Ihrem Zertifikat zugeordnet ist.

Anmerkung: Wenn Sie über Netscape auf RA Desktop zugreifen, und das System über eine längere Zeit hinweg keine Operationen ausführt, werden Sie von Netscape erneut zur Angabe Ihres Zertifikats aufgefordert. Durch diese zusätzliche Sicherheitsfunktion wird Ihr Unternehmen geschützt, wenn Sie durch einen Notfall Ihren Arbeitsplatz verlassen müssen, ohne RA Desktop zuvor abzumelden.

Arbeiten mit Abfragen

Wählen Sie die Registerkarte **Abfrage** aus, um eine Abfrage vorzubereiten. Sie können diese Abfrage sehr spezifisch gestalten oder eine Gruppe mit Datensätzen abrufen, die über gemeinsame Merkmale verfügen. Sie können darüber hinaus die Anzahl der abzurufenden Datensätze begrenzen und angeben, wie viele auf einer Seite angezeigt werden sollen.

Übergeben einer Abfrage

Auf der Registerkarte **Abfrage** können Sie eine Abfrage vorbereiten zum Abrufen von Registrierungsanforderungen bzw. von Anforderungen für Schlüsselwiederherstellungen

sowie zum Abrufen von Zertifikatsdatensätzen, mit denen gearbeitet werden soll. Sie können die Abfrage auf der Basis des aktuellen Anforderungs- oder Zertifikatsstatus oder auf den Erneuerungs- oder Ablaufmerkmalen der Anforderungen bzw. Zertifikate aufbauen. Innerhalb dieser beiden Kategorien kann die Abfrage durch die Verwendung der anderen verfügbaren Felder weiter differenziert werden.

1. Verwenden Sie die Felder auf der Registerkarte, um die Abfrage vorzubereiten. Durch die Kombination einer beliebigen Anzahl der verfügbaren Felder können Sie anschließend Ihre Abfrage weiter differenzieren. Der Abschnitt „Abfragefelder" auf Seite 39 enthält eine Beschreibung der Felder.
   - Wenn Sie den Cursor über ein bestimmtes Feld bewegen, werden unten auf der Registerkarte Hilfetexte für dieses Feld angezeigt.
   - Sie können die Abfrage ausführen, ohne eigene Werte anzugeben. In diesem Fall werden die Datensätze aller anstehenden Anforderungen abgerufen, ohne dass hierbei die anderen Merkmale berücksichtigt werden.
2. Ändern Sie bei Bedarf den Grenzwert für die Anzahl der abzurufenden Datensätze.
3. Ändern Sie bei Bedarf die Anzahl der Datensätze, die auf einer Seite angezeigt werden, wenn Sie die Ergebnisse auf der Registerkarte **Ergebnisse** aufrufen.
4. Nach der Vorbereitung der Abfrage klicken Sie auf **Abfrage übergeben**.

   Während Sie auf die Abfrageergebnisse warten, wird ein Statusbalken angezeigt, der Sie über den Fortschritt der Abfrageverarbeitung informiert. Wenn die Ergebnisse Ihrer Abfrage vorliegen, wird die Registerkarte **Ergebnisse** automatisch angezeigt.
5. Die Registerkarte **Ergebnisse** enthält die Datensätze für die weitere Bearbeitung.

Zugehörige Abschnitte:

„Abrufen von anstehenden Zertifikatsanforderungen"
„Abrufen von anstehenden Schlüsselwiederherstellungsanforderungen"
„Abrufen von ablaufenden Zertifikaten" auf Seite 14
„Vordefinierte Abfragen" auf Seite 43

Abrufen von anstehenden Zertifikatsanforderungen

Führen Sie auf der Registerkarte **Abfrage** einen der folgenden Arbeitsschritte aus:

- Führen Sie eine Abfrage aus, ohne eigene Werte anzugeben. Diese Operation entspricht der Angabe des Status **Anstehend**.
- Geben Sie bei Bedarf, ohne die Auswahl unter **Abfrageart** zu ändern, zusätzliche Merkmale für die abzurufenden Datensätze an. Beispiel: Ihr Manager bittet Sie, die Registrierungsanforderung einer bestimmten Person vor anderen anstehenden Anforderungen zu bearbeiten. In diesem Fall können Sie in der Abfrage den Namen der gewünschten Person angeben.

Abrufen von anstehenden Schlüsselwiederherstellungsanforderungen

Auf der Registerkarte **Abfrage** können Sie eine anstehende Anforderung für Schlüsselwiederherstellung abrufen:

1. Wählen Sie unter **Abfrageart** die Option **Anhand von Wiederherstellungsstatus, Name und Aktualisierungsdatum** aus.
2. Wählen Sie unter **Schlüsselwiederherstellungsstatus** die Option **Anstehend** aus.

3. Klicken Sie auf **Abfrage übergeben**.

Zugehörige Abschnitte:

„Genehmigen einer Schlüsselwiederherstellungsanforderung” auf Seite 24
„Zurückweisen einer Schlüsselwiederherstellungsanforderung” auf Seite 25

Abrufen von ablaufenden Zertifikaten

Auf der Registerkarte **Abfrage** können Sie eine Abfrage zum Abrufen von Datensätzen erneuerbarer Zertifikate vorbereiten, deren Gültigkeit innerhalb eines bestimmten Zeitraums abläuft. Gehen Sie hierzu wie folgt vor:

1. Wählen Sie unter **Abfrageart** die Option **Anhand von Erneuerbarkeit und Ablaufdatum** aus.
2. Öffnen Sie die Liste unter **Erneuerbarkeit** und klicken Sie auf **Erneuerbar**.
3. Differenzieren Sie die Abfrage so, dass nur die Datensätze von Zertifikaten abgerufen werden, deren Gültigkeit während des gewünschten Zeitraums ausläuft. Führen Sie unter **Bereich der Ablaufdaten** folgende Arbeitsschritte aus:
   - Geben Sie das früheste Ablaufdatum ein oder wählen Sie den gewünschten Wert unter **Von** aus.
   - Geben Sie das späteste Ablaufdatum ein oder wählen Sie dieses unter **Bis** aus.

Zugehörige Abschnitte:

„Ändern eines Gültigkeitszeitraums” auf Seite 22

Auswählen eines Datums aus dem Kalender

Gehen Sie wie folgt vor, um ein Datum aus dem Kalender auszuwählen, anstatt den gewünschten Wert in ein Datumsfeld einzugeben:

1. Klicken Sie auf das kleine Kalendersymbol neben dem Textfenster des Felds.

   Daraufhin wird der Kalender geöffnet und zeigt den aktuellen Monat oder die Monatsangabe des Datums im Feld an.
2. Klicken Sie im Kalender auf das gewünschte Jahr, wenn Sie hier einen anderen Wert auswählen möchten. Daraufhin wird eine Liste der Jahre angezeigt, die ausgewählt werden können.
3. Wenn Sie einen Monat auswählen möchten, klicken Sie auf einen der Pfeile neben dem Namen des aktuellen Monats. Der Linkspfeil dient zur Anzeige von Monatsangaben vor dem aktuellen, der Rechtspfeil zur Anzeige von Monatsangaben nach dem aktuellen Monat.
4. Wenn Sie einen Tag auswählen möchten, klicken Sie auf den gewünschten Tag innerhalb des Monats.

   Der Kalender wird anschließend geschlossen und zeigt nun im Feld das ausgewählte Datum an.

Definieren eines Grenzwerts für die Anzahl von abzurufenden Datensätzen

Auf der Registerkarte **Abfrage** können Sie die Anzahl der Datensätze begrenzen, die abgerufen werden sollen. Dies gilt auch dann, wenn eine größere Anzahl von Datensätzen den Abfragekriterien entspricht. Der definierte Grenzwert wird nur für die von Ihnen vorbereitete Abfrage angewendet.

1. Öffnen Sie die Liste unter **Anzahl der abzurufenden Datensätze** und wählen Sie den gewünschten Grenzwert aus. Der Standardwert lautet 150.

   Durch diesen Grenzwert wird der Umfang der Abfrageergebnisse beeinflusst.

2. Geben Sie die restlichen Werte für Ihre Abfrage an.

Definieren der Anzahl von Sätzen pro Seite

Auf der Registerkarte **Abfrage** können Sie die Anzahl der Datensätze begrenzen, die auf einer Seite der Registerkarte **Ergebnisse** angezeigt werden sollen. Der definierte Grenzwert wird nur für die von Ihnen vorbereitete Abfrage angewendet.

1. Führen Sie unter **Sätze pro Seite** einen der folgenden Arbeitsschritte aus:

   - Öffnen Sie die Liste und wählen Sie den gewünschten Grenzwert aus.
   - Überschreiben Sie den angezeigten Standardwert mit einer numerischen Angabe.

   Dieser Wert steuert die Anzeige Ihrer Abfrage.

2. Geben Sie die restlichen Werte für Ihre Abfrage an.

Abrufen von Rückmeldungen während der Verarbeitung

Nachdem Sie auf einen Befehlsknopf einer beliebigen Registerkarte geklickt haben, wird im Statusbereich unten auf der Anzeige der Fortschritt der von Ihnen angeforderten Verarbeitungsoperation angezeigt.

Arbeiten mit Ergebnissen

Wählen Sie die Registerkarte **Ergebnisse** aus, um die Ergebnisse Ihrer Abfrage anzuzeigen.

Auf der Registerkarte können mehrere abgerufene Datensätze angezeigt werden. Die Anzahl der Datensätze pro Seite hängt von dem Wert ab, der bei der Übergabe der Abfrage ausgewählt wurde.

Anzeigen von Abfrageergebnissen

Auf der Registerkarte **Ergebnisse** können Sie nach der Ausführung einer Abfrage die Ergebnisse anzeigen.

Jede Zeile der Tabelle unter **Abfrageergebnisse** enthält einen Datensatz, der mit den definierten Abfragekriterien übereinstimmt. Für die Abfragearten **Anhand von Anforderungsstatus, Name und Aktualisierungsdatum** und **Anhand von Erneuerbarkeit und Ablaufdatum** enthält die Tabelle die folgenden Spalten:

Name Der Name, der einer Anforderung oder einem Zertifikat zugeordnet wurde. Dieser Name wird im Format *nachname, vorname* angezeigt.

Anforderungsstatus
Der aktuelle Status der Registrierungsanforderung, z. B. ″Genehmigt″. Der Abschnitt „Status der Registrierungsanforderungen” auf Seite 51 enthält eine Beschreibung der verschiedenen Statuswerte.

Ausführungsstatus
Der aktuelle Status der Anforderungsverarbeitung, z. B. ″Übergeben″.

Sicherungsstatus
Der aktuelle Status der Schlüsselsicherungsanforderung.

Zuletzt aktualisiert
Das Datum, das dem Anforderungs- oder Zertifikatsstatus zugeordnet ist.

Empfangsdatum
Das Datum, zu dem die Registrierungsanforderung empfangen wurde.

Für die Abfrageart **Anhand von Wiederherstellungsstatus, Name und Aktualisierungsdatum** enthält die Tabelle die folgenden Spalten:

Name Der Name, der einer Anforderung oder einem Zertifikat zugeordnet wurde. Dieser Name wird im Format *nachname, vorname* angezeigt.

Ausführungsstatus
Der aktuelle Status der Anforderungsverarbeitung, z. B. ″Übergeben″.

Sicherungsstatus
Der aktuelle Status der Schlüsselsicherungsanforderung.

Wiederherstellungsstatus
Der aktuelle Status der Schlüsselwiederherstellungsanforderung.

Zuletzt aktualisiert
Das Datum, das dem Anforderungs- oder Zertifikatsstatus zugeordnet ist.

Empfangsdatum
Das Datum, zu dem die Registrierungsanforderung empfangen wurde.

Gehen Sie wie folgt vor, um die Abfrageergebnisse anzuzeigen:

1. Suchen Sie die benötigten Datensätze. Hierzu können Sie einen der folgenden Arbeitsschritte ausführen:
   - Blättern Sie in der Tabelle, führen Sie eine Größenanpassung der Spalten durch oder sortieren Sie die Zeilen der Tabelle.
   - Blättern Sie von Seite zu Seite, um mehr Ergebnisdaten anzuzeigen.
2. Wenn Sie die gewünschten Datensätze gefunden haben, können Sie bei Bedarf die folgenden Aktionen ausführen:
   - Wählen Sie einen oder mehrere Datensätze aus und behandeln Sie diese als Gruppe.
   - Wählen Sie einen bestimmten Datensatz für die detailliertere Anzeige aus.

Anmerkung: Wenn der benötigte Datensatz nicht abgerufen werden konnte, rufen Sie die Registerkarte **Abfrage** erneut auf:

- Wenn die Abfrage nicht korrekt war, führen Sie die erforderlichen Änderungen durch und wiederholen Sie die Operation.

- Wenn die Abfrage korrekt war, definieren Sie die Anzahl der abzurufenden Datensätze so, dass eine höhere Anzahl von Datensätzen abgerufen wird, und wiederholen anschließend die Operation.

Zugehörige Abschnitte:

„Definieren der Anzahl von Sätzen pro Seite" auf Seite 15

Anzeigen von Ergebnissen auf mehreren Seiten

Auf der Registerkarte **Ergebnisse** können die Ergebnisse Ihrer Abfrage mehrere Seiten in Anspruch nehmen. Die Anzahl der Seiten hängt von der Anzahl der Datensätze, die mit Ihren Abfragekriterien übereinstimmen, sowie von der für die Anzeige definierten Seitengröße ab. Der Statusbereich enthält Informationen zur Anzahl der verfügbaren Seiten und zur aktuellen Position innerhalb dieser Seitenfolge.

- Klicken Sie auf **Nächste Seite**, um die nächste Seite innerhalb der Seitengruppe aufzurufen.
- Klicken Sie auf **Vorhergehende Seite**, um die vorangegangene Seite innerhalb der Seitengruppe aufzurufen.
- Wenn Sie um mehrere Seiten zurückblättern möchten, ist es möglicherweise schneller, zur Registerkarte **Abfrage** zurückzukehren und die Abfrage dort erneut zu übergeben. In diesem Fall wird auf der Registerkarte **Ergebnisse** die erste Seite der Abfrageergebnisse erneut angezeigt.

Anzeigen von Details eines Elements

Führen Sie auf der Registerkarte **Ergebnisse** die folgenden Schritte aus:

1. Wählen Sie in der Tabelle der Abfrageergebnisse die Zeile eines Datensatzes aus den Abfrageergebnissen aus.
2. Klicken Sie auf **Details anzeigen**.

   Daraufhin wird automatisch die Registerkarte **Details** aufgerufen, um die Details des ausgewählten Datensatzes anzuzeigen.
3. Wählen Sie auf der Registerkarte **Details** unter **Anzeigen** die Detailart aus, die angezeigt werden soll.

Anmerkung: Sie können die Details eines Datensatzes auch anzeigen, indem Sie auf der Registerkarte **Ergebnisse** doppelt auf diesen Datensatz klicken oder indem Sie den Datensatz und anschließend die Registerkarte **Details** auswählen.

Zugehörige Abschnitte:

„Ausführen von Aktionen für einzelne Datensätze" auf Seite 21

Anzeigen der Attribute von Elementen

Führen Sie auf der Registerkarte **Ergebnisse** die folgenden Schritte aus:

1. Wählen Sie aus der Tabelle der Abfrageergebnisse den gewünschten Datensatz aus.
2. Klicken Sie auf **Details anzeigen**, um eine detailliertere Anzeige des ausgewählten Datensatzes auf der Registerkarte **Details** aufzurufen.

3. Wählen Sie auf der Registerkarte **Details** unter **Anzeigen** den Typ der Attribute aus, die angezeigt werden sollen. Der Abschnitt „Detailgruppen” auf Seite 50 enthält eine Beschreibung zur Gruppierung der verfügbaren Attribute. Der Standardwert lautet **Basisattribute**.
4. Prüfen Sie die Tabelle.

   Jede Zeile der Tabelle enthält ein Attribut der Anforderung bzw. des Zertifikats. Der Abschnitt „Attribute von Anforderungen und Zertifikaten” auf Seite 47 enthält eine Beschreibung der Anforderungsattribute. Die Tabelle verfügt über die folgenden Spalten:

   Attributname
   Der Name des Attributs.

   Attributwert
   Der Wert des Attributs. Dieser kann sich während der Gültigkeitsdauer einer Anforderung oder eines Zertifikats ändern.
5. Blättern Sie in der Tabelle, führen Sie eine Größenanpassung der Spalten durch oder sortieren Sie bei Bedarf die Zeilen der Tabelle.

Zugehörige Abschnitte:

„Ändern eines Attributwerts” auf Seite 22

Anzeigen von Aktionsprotokollen

Führen Sie auf der Registerkarte **Ergebnisse** die folgenden Schritte aus:

1. Wählen Sie aus der Tabelle der Abfrageergebnisse den gewünschten Datensatz aus.
2. Klicken Sie auf **Details anzeigen**, um eine detailliertere Anzeige des ausgewählten Datensatzes auf der Registerkarte **Details** aufzurufen.
3. Wählen Sie auf der Registerkarte **Details** unter **Anzeigen** die Option **Aktionsprotokoll** aus.
4. Prüfen Sie die Tabelle. Sie enthält Details zu allen Ereignissen, die innerhalb der Gültigkeitsdauer des ausgewählten Elements auftreten.

   Jede Zeile im Aktionsprotokoll beschreibt eine Aktion, die für das Element ausgeführt wurde. Die aufgezeichneten Daten umfassen das Datum des Ereignisses, die verantwortliche Person oder Einheit und alle zugehörigen Kommentare. Die Tabelle verfügt über die folgenden Spalten:

   Datum
   Das Datum der Aktion, die in derselben Zeile angezeigt wird.

   Von Der registrierte Name des Registrators, der die Aktion ausgeführt hat, oder der Name des entsprechenden RA-Programms.

   Anforderungsstatus
   Der Status der Registrierungsanforderung, z. B. ″Genehmigt″. Der Abschnitt „Status der Registrierungsanforderungen” auf Seite 51 enthält eine Beschreibung der verschiedenen Statuswerte.

   Ausführungsstatus
   Der Status der Anforderungsverarbeitung, z. B. ″Übergeben″.

Kommentar

Der Kommentar, der vom Registrator bei der Ausführung der Aktion angegeben wurde.

5. Blättern Sie in der Tabelle, führen Sie eine Größenanpassung der Spalten durch oder sortieren Sie bei Bedarf die Zeilen der Tabelle.

Zugehörige Abschnitte:

„Aktionsprotokoll - Ereignisse” auf Seite 47

Wechseln zwischen Registerkarten

In bestimmten Fällen wechseln Sie automatisch von einer Registerkarte zur anderen. Beispiel:

- Wenn Sie von der Registerkarte **Abfrage** aus eine Abfrage ausführen, wechseln Sie zur Registerkarte **Ergebnisse**, sobald die Abfrageergebnisse in RA Desktop vorliegen.
- Wenn Sie Details zu einem Datensatz anfordern, wechseln Sie zur Registerkarte **Details**.
- Wenn Sie eine Aktion auf der Registerkarte **Details** abschließen, wechseln Sie erneut zu den Abfrageergebnissen auf der Registerkarte **Ergebnisse**.

Wenn Sie in anderen Situationen zu einer anderen Registerkarte wechseln möchten, klicken Sie einfach auf die gewünschte Registerkarte. Anschließend führt das System folgende Operationen aus:

- Wenn Sie nach der Anzeige der Abfrageergebnisse zur Registerkarte **Abfrage** zurückkehren, wird die Abfrage weiterhin angezeigt.
- Wenn Sie Details zu einem falschen Datensatz anfordern, können Sie die Abfrageergebnisse auf der Registerkarte **Ergebnisse** erneut aufrufen. Dort können Sie dann einen anderen Datensatz auswählen und für diesen Details aufrufen. Die Abfrageergebnisse bleiben auf der Registerkarte **Ergebnisse** erhalten, bis Sie eine weitere Abfrage ausführen.
- Wenn Sie zur Registerkarte **Details** wechseln, nachdem Sie einen Datensatz auf der Registerkarte **Ergebnisse** ausgewählt haben, enthält die Registerkarte **Details** diesen Datensatz. Die Registerkarte enthält keine Informationen, wenn auf der Registerkarte **Ergebnisse** kein Datensatz oder mehr als ein Datensatz ausgewählt wurde. Nach der Übergabe einer Aktion auf der Registerkarte **Details** werden die Informationen auf der Seite dieser Registerkarte gelöscht.

Anmerkung: Wenn Sie eine Sitzung starten, werden in den Feldern von RA Desktop nur die Standardwerte angezeigt.

Anpassen der Größe von Tabellenspalten

Gehen Sie wie folgt vor, um die Größe einer Tabellenspalte anzupassen:

1. Platzieren Sie den Cursor auf dem Rand der Spalte, deren Größe angepasst werden soll.
2. Klicken Sie mit der Maus und ziehen Sie diese nach links oder rechts, um die Spaltenbreite zu ändern.
3. Lassen Sie die Maustaste wieder los, wenn die Spalte die gewünschte Breite aufweist.

Sortieren von Tabellenzeilen nach bestimmten Spalten

Gehen Sie wie folgt vor, um Tabellenzeilen nach einer bestimmten Spalte zu sortieren:

- Klicken Sie auf die Spaltenüberschrift.
- Klicken Sie noch einmal, wenn Sie die Sortierrichtung ändern möchten.

Auswählen von Datensätzen in Tabellen

Sie können einen oder mehrere Datensätze auswählen. Gehen Sie hierzu wie folgt vor:

- Um einen einzelnen Datensatz auszuwählen, klicken Sie auf die zugehörige Zeile.
- Um mehrere benachbarte Datensätze auszuwählen, klicken Sie auf den ersten Datensatz der gewünschten Gruppe. Halten Sie die **Umschalttaste** gedrückt und klicken Sie dann bei weiterhin gedrückter Umschalttaste auf den letzten Datensatz der Gruppe.
- Wenn Sie mehrere Datensätze auswählen möchten, die nicht direkt aufeinander folgen, halten Sie die **Steuerungstaste** gedrückt, während Sie alle gewünschten Datensätze anklicken.
- Wenn Sie die Auswahl eines Datensatzes zurücknehmen möchten, klicken Sie ihn erneut an.

Ausführen von Aktionen

Sie können eine Aktion für eine Registrierungsanforderung ausführen oder den Datensatz eines Zertifikats aktualisieren. Sowohl die Registerkarte **Ergebnisse** als auch die Registerkarte **Details** enthalten Felder für die Auswahl der gewünschten Aktion. Die möglichen Aktionen sind von den eigenen Berechtigungen in der Registrierungsdomäne abhängig, in der Sie als Registrator definiert sind.

Ausführen von Aktionen für mehrere Datensätze

Auf der Registerkarte **Ergebnisse** stellt jede Zeile in der Tabelle einen Datensatz in den Abfrageergebnissen dar. Sie können Aktionen für einen oder mehrere der Datensätze einer Tabelle ausführen oder einen Datensatz genauer prüfen, bevor Sie die gewünschte Aktion ausführen.

- Gehen Sie wie folgt vor, um eine Aktion auszuführen, während mehrere Datensätze angezeigt werden:

  1. Wählen Sie einen oder mehrere Datensätze aus.
  2. Geben Sie bei Bedarf unter **Definition des Gültigkeitszeitraums** einen Gültigkeitszeitraum für das aktive Zertifikat an.
  3. Geben Sie bei Bedarf unter **Wählen Sie das Anforderungsprofil aus** ein anderes Anforderungsprofil für eine Anforderung an, die momentan genehmigt wird. Der Abschnitt „Gelieferte Zertifikatstypen” auf Seite 49 enthält eine Beschreibung der Merkmale der Zertifikate, die den einzelnen Anforderungsprofilen zugeordnet sind.
  4. Öffnen Sie die Liste unter **Führen Sie eine Aktion für die ausgewählten Elemente aus** bzw. **Führen Sie eine Aktion für das angezeigte Element aus** und wählen Sie die gewünschte Aktion aus. Die einzigen Aktionen, die für Sie zur Verfügung stehen, sind die Berechtigungen für das Arbeiten mit Datensätzen.
  5. Wenn Sie als Aktion **Widerrufen** auswählen, müssen Sie auch eine entsprechende Begründung angeben. Öffnen Sie die Liste unter **Begründung für den Widerruf**

und wählen Sie die gewünschte Begründung aus. Der Abschnitt „Gründe für das Widerrufen eines Zertifikats” auf Seite 46 enthält eine Beschreibung der Bedeutung der verschiedenen Begründungen.

6. Geben Sie bei Bedarf unter **Geben Sie einen Kommentar zur ausgeführten Aktion ein** einen Kommentar zur Dokumentierung Ihrer Aktion ein.
7. Klicken Sie auf **Aktion übergeben**, um die Aktion für die ausgewählten Datensätze zu übergeben.

- Gehen Sie wie folgt vor, um vor der Ausführung einer Aktion weitere Details eines Datensatzes anzuzeigen:
  1. Wählen Sie die Zeile aus, in der sich der Datensatz befindet.
  2. Klicken Sie auf den Knopf **Details anzeigen**.

Zugehörige Abschnitte:

„Anpassen der Größe von Tabellenspalten” auf Seite 19
„Sortieren von Tabellenzeilen nach bestimmten Spalten” auf Seite 20

Ausführen von Aktionen für einzelne Datensätze

Auf der Registerkarte **Details** können Sie weitere Änderungen für den angezeigten Datensatz vornehmen, bevor eine Aktion angegeben wird:

1. Wählen Sie unter **Anzeigen** den Typ der Details aus, die angezeigt werden sollen.
   Wenn Sie die Verarbeitungsattribute eines Elementes anzeigen, können einige der Werte in der Tabelle geändert werden.
2. Ändern Sie die Attributwerte entsprechend Ihren individuellen Anforderungen. Der Abschnitt „Attribute von Anforderungen und Zertifikaten” auf Seite 47 enthält eine Beschreibung der verschiedenen Attribute.
3. Geben Sie bei Bedarf unter **Definition des Gültigkeitszeitraums** einen Gültigkeitszeitraum für das aktive Zertifikat an.
4. Geben Sie bei Bedarf unter **Wählen Sie das Anforderungsprofil aus** ein anderes Anforderungsprofil für eine Anforderung an, die momentan genehmigt wird. Der Abschnitt „Gelieferte Zertifikatstypen” auf Seite 49 enthält eine Beschreibung der Merkmale der Zertifikate, die den einzelnen Anforderungsprofilen zugeordnet sind.
5. Öffnen Sie die Liste unter **Aktion für das angezeigte Element ausführen** und wählen Sie die gewünschte Aktion aus. Die einzigen Aktionen, die für Sie zur Verfügung stehen, sind die Berechtigungen für das Arbeiten mit Datensätzen.

   Anmerkung: Wenn Sie als Aktion **Widerrufen** auswählen, müssen Sie auch die Begründung für den Widerruf auswählen. Der Abschnitt „Gründe für das Widerrufen eines Zertifikats” auf Seite 46 enthält eine Beschreibung zu den zulässigen Begründungen.
6. Geben Sie bei Bedarf unter **Geben Sie einen Kommentar zur ausgeführten Aktion ein** einen Kommentar zur Dokumentierung Ihrer Aktion ein.
7. Klicken Sie auf **Aktion übergeben**, um die Aktion zu übergeben.

Zugehörige Abschnitte:

„Anpassen der Größe von Tabellenspalten” auf Seite 19
„Sortieren von Tabellenzeilen nach bestimmten Spalten” auf Seite 20

Ändern eines Attributwerts

Auf der Registerkarte **Details** können Sie bei der Genehmigung einer Registrierungsanforderung oder der Ausführung einer Aktion für eine Ausführungsanforderung die Werte bestimmter Attribute ändern. Gehen Sie hierzu wie folgt vor:

1. Wählen Sie unter **Anzeigen** die Option **Verarbeitungsattribute** aus.
2. Blättern Sie bis zu dem Attribut, das aktualisiert werden soll.

   Die Werte, die aktualisiert werden können, verfügen entweder über ein Textfenster zur Eingabe eines neuen Wertes oder ein Listenfenster zur Auswahl anderer Werte. Der Abschnitt „Attribute von Anforderungen und Zertifikaten” auf Seite 47 enthält eine Beschreibung der verschiedenen Attribute.
3. Geben Sie den gewünschten Wert ein oder wählen Sie ihn aus der Liste aus.

Anmerkung: Die Werte im Anforderungsprofil können die von Ihnen definierten Werte überschreiben.

Ändern eines Gültigkeitszeitraums

Auf der Registerkarte **Ergebnisse** bzw. **Details** können Sie den Gültigkeitszeitraum für das Zertifikat ändern, wenn Sie eine Registrierungsanforderung genehmigen oder eine ausgeführte Anforderung bearbeiten. Geben Sie unter **Definition des Gültigkeitszeitraums** den gewünschten Datumsbereich an. Um ein Datum anzugeben, klicken Sie auf den Kalender, um diesen zu öffnen, und anschließend auf das gewünschte Datum. Wenn Sie das Datum eingeben, verwenden Sie beim Ausfüllen des Textfensters dasselbe Format, das auch im Kalender benutzt wird.

- Geben Sie unter **Anfangsdatum** das Datum an, an dem die Gültigkeit des Zertifikats beginnen soll.
- Geben Sie unter **Enddatum** das Datum an, an dem die Gültigkeit des Zertifikats ablaufen soll.

Der von Ihnen angegebene Gültigkeitszeitraum wird an die RA weitergeleitet, wenn Sie die Aktion übergeben.

Richtlinien für die Verwendung:

Der Gültigkeitszeitraum für ein Zertifikat kann so geändert werden, dass er innerhalb der Begrenzung des definierten Anforderungsprofils liegt. Wenn ein Benutzer beispielsweise ein Zertifikat mit einem Gültigkeitszeitraum von einem Jahr anfordert, können Sie diesen Zeitraum auf weniger als ein Jahr verkürzen. Soll der Gültigkeitszeitraum dagegen über die durch das Profil definierte Begrenzung hinaus erweitert werden, müssen Sie eine der folgenden Aktionen ausführen:

- Weisen Sie das Zertifikat zurück und fordern Sie den Benutzer auf, eine Anforderung zu übergeben, in der ein längerer Gültigkeitszeitraum, beispielsweise 2 Jahre, für das Zertifikat angegeben ist.

- Ändern Sie das Anforderungsprofil und übergeben Sie die Änderung. Dabei müssen Sie die Aktion **Als 'anstehend' behalten** auswählen, bis alle Änderungen ausgeführt sind.

  Gehen Sie beispielsweise wie folgt vor, wenn Sie für ein Zertifikat den Zertifikatstyp von einem 1-Jahres-Zertifikat in ein 2-Jahres-Zertifikat ändern und gleichzeitig den Gültigkeitszeitraum für das Zertifikat auf 18 Monate begrenzen möchten:

  1. Wählen Sie die Zertifikatsanforderung aus und ändern Sie den Zertifikatstyp in ein 2-Jahres-Zertifikat.
  2. Wählen Sie **Als 'anstehend' behalten** aus und klicken Sie anschließend auf **Aktion übergeben**.
  3. Wählen Sie die Zertifikatsanforderung erneut aus und ändern Sie das Start- und Enddatum so, dass der Gültigkeitszeitraum auf 18 Monate begrenzt ist.
  4. Wählen Sie **Genehmigen** aus und klicken Sie anschließend auf **Aktion übergeben**.

Angeben des Anforderungsprofils

Auf der Registerkarte **Ergebnisse** bzw. **Details** können Sie angeben, dass ein anderes Anforderungsprofil für die Zertifikatserstellung verwendet werden soll, wenn Sie eine Registrierungsanforderung genehmigen.

Wählen Sie unter **Wählen Sie das Anforderungsprofil aus** eine der folgenden Optionen aus:

- Wählen Sie in der Liste das gewünschte Anforderungsprofil aus. Alle Profile in der Liste können angegeben werden. Der Abschnitt „Gelieferte Zertifikatstypen" auf Seite 49 enthält eine Beschreibung der Zertifikate, die den einzelnen Anforderungsprofilen zugeordnet sind.
- Wählen Sie **Aktuellen Standardwert verwenden** aus. Dies ist der Standardwert. Mit dieser Einstellung können Sie auch dann weiterarbeiten, wenn das aktuelle Profil nicht zu den Profilen gehört, zu deren Angabe Sie berechtigt sind.

Das von Ihnen angegebene Profil wird zur Verarbeitung der Anforderung und zum Erstellen des Zertifikates nach der Übergabe der Aktion verwendet.

Hinzufügen eines Kommentars

Auf der Registerkarte **Ergebnisse** bzw. **Details** können Sie Kommentare zur Erläuterung der ausgeführten Aktion hinzufügen:

1. Wählen Sie unter **Führen Sie eine Aktion für die ausgewählten Elemente aus** bzw. **Führen Sie eine Aktion für das angezeigte Element aus** eine Aktion aus.
2. Geben Sie unter **Geben Sie einen Kommentar zur ausgeführten Aktion ein** einen Kommentar im Textfenster ein. Sie können maximal 512 Zeichen eingeben.
3. Klicken Sie auf **Aktion übergeben**, um den Kommentar bei der Aktualisierung des Datensatzes einzubinden.

Der Kommentar wird zum Datensatz hinzugefügt, wenn Sie die Aktion übergeben.

Genehmigen einer Anforderung

Sie können eine Anforderung auf der Registerkarte **Ergebnisse** oder der Registerkarte **Details** genehmigen.

- Wenn Sie die Registerkarte **Ergebnisse** verwenden, können Sie mehrere Datensätze zur Genehmigung auswählen.
- Wenn Sie die Registerkarte **Details** verwenden, können Sie die Werte bestimmter Attribute ändern, bevor Sie die angezeigte Anforderung genehmigen.

Gehen Sie auf beiden Registerkarten wie folgt vor:

1. Klicken Sie unter **Führen Sie eine Aktion für die ausgewählten Elemente aus** bzw. **Führen Sie eine Aktion für das angezeigte Element aus** auf **Genehmigen**.
2. Klicken Sie auf **Aktion übergeben**.

Genehmigen einer Schlüsselwiederherstellungsanforderung

Sie können eine Schlüsselwiederherstellungsanforderung auf der Registerkarte **Ergebnisse** oder der Registerkarte **Details** genehmigen. Wenn Sie die Registerkarte **Ergebnisse** verwenden, können Sie mehrere Datensätze für die Genehmigung auswählen.

Gehen Sie auf beiden Registerkarten wie folgt vor:

1. Klicken Sie unter **Führen Sie eine Aktion für die ausgewählten Elemente aus** bzw. **Führen Sie eine Aktion für das angezeigte Element aus** auf **Schlüsselwiederherstellung genehmigen**.
2. Klicken Sie auf **Aktion übergeben**.

Behalten einer Anforderung im Status ″anstehend″

Sie können eine Anforderung auf der Registerkarte **Ergebnisse** oder auf der Registerkarte **Details** als ’anstehend’ behalten. Wenn Sie die Registerkarte **Ergebnisse** verwenden, können Sie mehrere Datensätze auswählen, die als ’anstehend’ behalten werden sollen.

Gehen Sie auf beiden Registerkarten wie folgt vor:

1. Klicken Sie unter **Führen Sie eine Aktion für die ausgewählten Elemente aus** bzw. **Führen Sie eine Aktion für das angezeigte Element aus** auf **Als ″anstehend″ behalten**.
2. Klicken Sie auf **Aktion übergeben**.

Zurückweisen einer Anforderung

Sie können eine Anforderung auf der Registerkarte **Ergebnisse** oder auf der Registerkarte **Details** zurückweisen. Wenn Sie die Registerkarte **Ergebnisse** verwenden, können Sie mehrere Datensätze für die Zurückweisung auswählen.

Gehen Sie auf beiden Registerkarten wie folgt vor:

1. Klicken Sie unter **Führen Sie eine Aktion für die ausgewählten Elemente aus** bzw. **Führen Sie eine Aktion für das angezeigte Element aus** auf **Zurückweisen**.
2. Klicken Sie auf **Aktion übergeben**.

Zurückweisen einer Schlüsselwiederherstellungsanforderung

Sie können eine Schlüsselwiederherstellungsanforderung auf der Registerkarte **Ergebnisse** oder der Registerkarte **Details** zurückweisen. Wenn Sie die Registerkarte **Ergebnisse** verwenden, können Sie mehrere Datensätze für die Zurückweisung auswählen.

Gehen Sie auf beiden Registerkarten wie folgt vor:

1. Klicken Sie unter **Führen Sie eine Aktion für die ausgewählten Elemente aus** bzw. **Führen Sie eine Aktion für das angezeigte Element aus** auf **Schlüsselwiederherstellung zurückweisen**.
2. Klicken Sie auf **Aktion übergeben**.

Ändern der Erneuerbarkeit

Sie können die Erneuerbarkeit eines Zertifikats auf der Registerkarte **Ergebnisse** oder auf der Registerkarte **Details** ändern. Sie können ein erneuerbares Zertifikat als nicht erneuerbar definieren und umgekehrt. Wenn Sie die Registerkarte **Ergebnisse** verwenden, können Sie mehrere Datensätze auswählen und die Erneuerbarkeit für die gesamte Gruppe ändern.

Gehen Sie auf beiden Registerkarten wie folgt vor:

1. Klicken Sie unter **Führen Sie eine Aktion für die ausgewählten Elemente aus** bzw. **Führen Sie eine Aktion für das angezeigte Element aus** auf eine der folgenden Optionen:
   - **Anforderung als ″erneuerbar″ definieren**
   - **Anforderung als ″nicht erneuerbar″ definieren**
2. Klicken Sie auf **Aktion übergeben**.

Aussetzen eines Zertifikats

Sie können ein Zertifikat auf der Registerkarte **Ergebnisse** oder auf der Registerkarte **Details** aussetzen. Wenn Sie die Registerkarte **Ergebnisse** verwenden, können Sie mehrere Zertifikate auswählen, die ausgesetzt werden sollen.

Gehen Sie auf beiden Registerkarten wie folgt vor:

1. Klicken Sie unter **Führen Sie eine Aktion für die ausgewählten Elemente aus** bzw. **Führen Sie eine Aktion für das angezeigte Element aus** auf **Zertifikat aussetzen**.

   Anmerkung: Sie können das Zertifikat zu einem späteren Zeitpunkt wieder aufnehmen. Nach Ablauf seiner Karenzzeit kann das betreffende Zertifikat jedoch nicht wieder aufgenommen werden.
2. Klicken Sie auf **Aktion übergeben**.

Zugehörige Abschnitte:

„Wiederaufnehmen eines Zertifikats” auf Seite 26

Widerrufen eines Zertifikats

Sie können ein Zertifikat auf der Registerkarte **Ergebnisse** oder auf der Registerkarte **Details** widerrufen. Wenn Sie die Registerkarte **Ergebnisse** verwenden, können Sie mehrere Zertifikate für den Widerruf auswählen.

Vor dem Widerrufen eines Zertifikats müssen Sie anhand der Registerkarte **Details** den Gültigkeitszeitraum für das Zertifikat überprüfen. Vergewissern Sie sich, dass das Zertifikat momentan gültig ist, bevor Sie die Anforderung für den Widerruf übergeben.

Gehen Sie auf beiden Registerkarten wie folgt vor, um ein Zertifikat zu widerrufen:

1. Klicken Sie unter **Führen Sie eine Aktion für die ausgewählten Elemente aus** bzw. **Führen Sie eine Aktion für das angezeigte Element aus** auf **Widerrufen**.
2. Wählen Sie unter **Begründung** eine Begründung aus.
3. Klicken Sie auf **Aktion übergeben**.

Nach der Ausführung dieser Aktion werden die Verarbeitungsattribute des Datensatzes aktualisiert. Das Attribut für die Widerrufbegründung wird auf den von Ihnen angegebenen Wert gesetzt.

Zugehörige Abschnitte:

„Aussetzen eines Zertifikats” auf Seite 25
„Wiederaufnehmen eines Zertifikats”

Wiederaufnehmen eines Zertifikats

In einem der folgenden Fälle kann es erforderlich sein, ein Zertifikat in der CRL wieder aufzunehmen:

- Bereinigung der CRL von Zertifikaten, die nicht mehr gültig sind.
- Reaktivierung eines Zertifikats, das zuvor ausgesetzt wurde.

  Anmerkung: Wenn der Gültigkeitszeitraum des Zertifikates in der Zwischenzeit abgelaufen ist, kann es nicht mehr reaktiviert werden.

Da keine Mitteilung über die Reaktivierung eines Zertifikats versendet wird, muss eine entsprechende Mitteilung per E-Mail oder auf einem anderen Korrespondenzweg gesendet werden.

Sie können ein Zertifikat aus der CRL auf der Registerkarte **Ergebnisse** oder auf der Registerkarte **Details** wieder aufnehmen. Wenn Sie die Registerkarte **Ergebnisse** verwenden, können Sie mehrere Zertifikate auswählen, die reaktiviert werden sollen.

Gehen Sie auf beiden Registerkarten wie folgt vor:

1. Klicken Sie unter **Führen Sie eine Aktion für die ausgewählten Elemente aus** bzw. **Führen Sie eine Aktion für das angezeigte Element aus** auf **Zertifikat wieder aufnehmen**.
2. Klicken Sie auf **Aktion übergeben**.

Zugehörige Abschnitte:

„Aussetzen eines Zertifikats” auf Seite 25

Publizieren eines Zertifikats

Sie können ein Zertifikat auf der Registerkarte **Ergebnisse** oder auf der Registerkarte **Details** für das Verzeichnis publizieren. Wenn Sie die Registerkarte **Ergebnisse** verwenden, können Sie mehrere Zertifikate publizieren.

Gehen Sie auf beiden Registerkarten wie folgt vor:

1. Klicken Sie unter **Führen Sie eine Aktion für die ausgewählten Elemente aus** bzw. **Führen Sie eine Aktion für das angezeigte Element aus** auf **Zertifikat publizieren**.

Anmerkung: Diese Aktion ist für Fälle gedacht, in denen die normale automatische Publizierung beim Ausstellen des Zertifikats fehlschlägt.

Prüfen der Berechtigungen für die Domäne

Führen Sie auf der Registerkarte **Ergebnisse** bzw. auf der Registerkarte **Details** folgende Schritte aus:

1. Klicken Sie auf **Führen Sie eine Aktion für die ausgewählten Elemente aus** bzw. **Führen Sie eine Aktion für das angezeigte Element aus**.
2. Prüfen Sie die Liste der Aktionen.

Diese Liste gibt die Aktionen an, die Sie gemäß Ihren Berechtigungen beim Arbeiten mit Datensätzen für Zertifikate und Registrierungsanforderungen in Ihrer Registrierungsdomäne ausführen dürfen. Wenn Sie lediglich über die Berechtigung verfügen, die Datensätze anzuzeigen, wird als einziger Wert in der Liste die Option **Keine Aktion verfügbar** angezeigt.

Beenden von RA Desktop

Gehen Sie wie folgt vor, um RA Desktop von einer der Registerkarten aus zu verlassen:

- Klicken Sie auf **Beenden**.

  Sie kehren damit zu der Web-Seite zurück, über die Sie auf RA Desktop zugegriffen haben, es sei denn, in Ihrem Unternehmen wurde ein anderer Pfad definiert.

- Schließen Sie den Desktop so wie ein herkömmliches Browser-Fenster. Klicken Sie hierzu auf eines der kleinen Symbole in der Titelleiste. Hierdurch wird der Browser geschlossen.

Deinstallieren von RA Desktop

Führen Sie die folgende Prozedur aus, wenn Sie das RA Desktop-Applet von der Workstation entfernen möchten:

1. Wählen Sie **Start → Einstellungen → Systemsteuerung** aus.
2. Klicken Sie doppelt auf **Software**.
3. Wählen Sie den Programmordner **IBM SecureWay Trust Authority RA Desktop** aus und klicken Sie auf **Hinzufügen/Entfernen**.
4. Wenn Sie dazu aufgefordert werden, das Löschen des Programms zu bestätigen, klicken Sie auf **Ja**.
5. Wird eine Nachricht angezeigt, in der mitgeteilt wird, dass bestimmte Ordner nicht gelöscht wurden, klicken Sie auf **Details**. Sie müssen alle im Fenster **Details** aufgeführten Ordner manuell löschen, um RA Desktop vollständig vom System zu entfernen.

4

Erläuterungen

Die Abschnitte in diesem Kapitel enthalten Definitionen und Beschreibungen zu den Konzepten, die sich auf die Registrierung, Zertifizierung und Verwaltung unter RA Desktop beziehen.

Registrierung

Bei der Registrierung wird ein Antrag für ein Zertifikat gestellt. Tivoli PKI bietet mehrere Registrierungsverfahren. Welche dieser Verfahren in Ihrem Unternehmen verfügbar sind, hängt von den Regeln ab, die definiert wurden. Benutzer können hierbei einen der folgenden Arbeitsschritte ausführen:

- Ausfüllen und Übergeben eines Tivoli PKI-Registrierungsformulars über den eingesetzten Web-Browser. In Standardinstallationen von Tivoli PKI befinden sich die Registrierungsformulare auf einer Web-Seite mit dem Namen ″Identitätsnachweis - Verwaltung″. An Ihrem Standort wird diese Seite möglicherweise unter einem anderen Namen aufgerufen.
- Durchführen einer informellen Vorabregistrierung und anschließend Angeben der entsprechenden Vorabregistrierungswerte in Tivoli PKI. Hierzu wird eine Tivoli PKI-Client-Anwendung verwendet, die auf der jeweiligen Workstation installiert ist.

Als RA-Registrator müssen Sie eine Registrierung für ein Zertifikat durchführen, mit dem Sie auf RA Desktop zugreifen können. Sie können dann zu einem späteren Zeitpunkt die Web-Seite für die Registrierung verwenden, um eine Vorabregistrierung für andere Benutzer durchzuführen.

Die Daten der Registrierungsformulare werden in Datenbanksätzen gespeichert, die über RA Desktop angezeigt werden können.

Vorabregistrierung

Tivoli PKI ermöglicht einem Programm oder Administrator die Vorabregistrierung zukünftiger Benutzer.

Im folgenden wird ein Szenario dargestellt, in dem beschrieben wird, wie Sie für andere Personen eine Vorabregistrierung für ein Zertifikat ausführen können:

- Sie müssen Informationen über die Person einholen, für die eine Vorabregistrierung ausgeführt werden soll. Sie können diese direkt von der betroffenen Person oder aus Datenbeständen des Unternehmens, z. B. aus entsprechenden Datenbanken, abfragen.
- Sie greifen über Ihren Web-Browser auf die Registrierungsseite zu. Dort finden Sie ein spezielles Registrierungsformular für Vorabregistrierungen.

- Sie füllen dieses Formular aus und geben hierbei Informationen zur Beschreibung der Person und zum gewünschten Zertifikatstyp an. Anschließend übergeben Sie das Formular.
- Sie prüfen den Status der Anforderung.

  Wenn der Antrag für die Vorabregistrierung genehmigt ist, erhalten Sie eine Transaktions-ID, ein Kennwort und die Webadresse der RA, die die Genehmigung der Anforderung durchgeführt hat.
- Sie leiten diese Informationen (per Telefon, E-Mail oder persönlich) an die Person weiter, für die die Vorabregistrierung ausgeführt wurde. Optional können Sie zur leichteren Verständlichkeit auch eine Vorabregistrierungsdatei an die registrierte Person versenden, die weitere Informationen zur Anforderung enthält. Die Person verwendet die von Ihnen gesendeten Daten, wenn sie für die Anforderung ihres Zertifikats bereit ist.

Weitere Informationen zur Ausführung von Vorabregistrierungsaufgaben enthält das *Tivoli PKI Benutzerhandbuch.*

Webbrowserunterstützung

Tivoli PKI ermöglicht die Erstellung einer Registrierungsanforderung. Hierzu wird über einen der folgenden Web-Browser ein Registrierungsformular ausgefüllt und übergeben:

- Microsoft Internet Explorer, ab Release 5.0.
- Netscape Navigator oder Netscape Communicator, nur Version 4.7*x*.

Sie können mit einem der folgenden Browser auf RA Desktop zugreifen:

- Microsoft Internet Explorer, ab Release 5.0
- Netscape Navigator oder Netscape Communicator, nur Version 4.7*x*.

Registrierung

Bei der Registrierung handelt es sich um einen Prozess zur Gewährung eines digitalen Zertifikats für eine Person oder eine andere Entität. Bei Tivoli PKI werden vor der Registrierung die Informationen, die mit der Registrierungsanforderung übergeben wurden, durch ein Programm oder einen Registrator ausgewertet. Anschließend und unabhängig davon, ob die Anforderung genehmigt wird, erstellt die Registrierungsstelle (RA) von Tivoli PKI einen Datensatz für die Anforderung. Dieser wird in der Registrierungsdatenbank gespeichert. Wird durch die zuständige Stelle das Zertifikat genehmigt, wird dieses vom Zertifikatsaussteller (CA) von Tivoli PKI ausgestellt.

Unternehmensregel

Wenn die Aufgaben des Registrators durch ein entsprechendes Programm ergänzt werden, werden die Unternehmensregeln des jeweiligen Unternehmens von diesem Programm für einen Teil der Registrierungsinformationen angewendet. Die auswertbaren Informationen sind weniger komplex als die Informationen, die von Ihnen ausgewertet werden können. Die Werte sind normalerweise präzise und geben z. B. die Anzahl der Jahre an, die eine Person bereits an einem bestimmten Wohnort lebt. Tivoli PKI ermöglicht Ihrem Unternehmen die Bereitstellung von Regelinformationen für ein solches Programm. Diese bilden dann die Basis für die Auswertungen.

Registrierungsstellen

Unter Tivoli PKI ist die Registrierungsstelle (RA) als Server-Anwendung implementiert. Sie dient zur Ausführung folgender Verwaltungsaufgaben, die bei der Registrierung von Benutzern ausgeführt werden müssen:

- Bestätigung der Identität des Benutzers
- Prüfung der Berechtigung der anfordernden Person für ein Zertifikat mit den gewünschten Attributen und Berechtigungen
- Genehmigung oder Zurückweisung von Anforderungen zur Erstellung oder zum Widerruf von Zertifikaten
- Aussetzung oder Reaktivierung von Zertifikaten
- Prüfung, ob Personen, die versuchen, auf eine gesicherte Anwendung zuzugreifen, über den passenden privaten Schlüssel verfügen, der dem öffentlichen Schlüssel eines Zertifikats zugeordnet ist.

Bei der Verwendung von RA Desktop initialisieren oder steuern Sie bestimmte Aktionen der RA von Tivoli PKI.

Registrierungsdatenbanken

In einer Registrierungsdatenbank von Tivoli PKI werden Registrierungssätze gespeichert. Bei der Registrierungsdatenbank handelt es sich um eine relationale Datenbank, die mit Hilfe von IBM DB2® Universal Database erstellt wird. Die Datensätze werden von Tivoli PKI verschlüsselt. Über RA Desktop kann ein entsprechend berechtigter Registrator jedoch die Mehrheit der Registrierungsinformationen lesen.

Registrierungsdomänen

Jedes Tivoli PKI-System verfügt über eine bestimmte Registrierungsdomäne. Diese Domäne definiert die Unternehmensregeln und Zertifikatsregeln sowie die Ressourcen, die für die Registrierung und die Zertifizierung in Ihrem Unternehmen festgelegt sind. Benutzer, die auf eine Ressource zugreifen möchten, müssen innerhalb der Domäne für die gewünschte Ressource registriert sein.

Wenn die RA-Server-Software installiert ist, umfasst diese die grundlegenden Komponenten, auf deren Basis ein Unternehmen eine Registrierungsfunktion installieren kann. Sie kann alle Sprachen oder Regeln verwenden, die von der RA unterstützt werden. Die Webadresse für den Zugriff auf die Registrierungsseiten Ihres Unternehmens besteht aus dem Domänennamen, der Sprache und dem Installationspfad.

Lautet beispielsweise der Name Ihres öffentlichen Webservers 'MyPublicWebServer' und der Domänenname 'MyDomain', können Sie über die folgende Webadresse auf die Registrierungsfunktion zugreifen:

```
http://MyPublicWebServer/MyDomain/index.jsp
```

Ein Tivoli PKI-System enthält eine Standard-Java-Server-Seite (Java Server Page, JSP), `index.jsp`. Diese Seite wird unter der Webadresse für die Registrierungsdomäne angezeigt. Sie bietet die folgenden Registrierungsservices:

- Zukünftige Benutzer verwenden diese Web-Seite, um ein Zertifikat anzufordern und um eigene Browser-Zertifikate zu erneuern oder zu widerrufen.

- Zur Unterstützung dieser Benutzer müssen Sie die Web-Seite aufrufen und ein eigenes Zertifikat für den Zugriff auf RA Desktop abrufen. Anschließend können Sie mit diesem Zertifikat eine Vorabregistrierung für andere Benutzer durchführen.

Sie greifen auf RA Desktop zu, um mit Registrierungsanforderungen und Zertifikaten zu arbeiten, die einer bestimmten Registrierungsdomäne zugeordnet sind.

Registrierungssätze

Jede Anforderung für ein Zertifikat ist ein Formular für die Registrierung, das an die Registrierungsstelle (RA) von Tivoli PKI übergeben wird. Für jede Registrierungsanforderung wird ein Datensatz in der Registrierungsdatenbank angelegt. Aktualisierungen an diesem Datensatz geben alle Aktionen wider, die für die Anforderung ausgeführt wurden. Dies gilt auch für eine Zurückweisung der Anforderung. Wenn ein Zertifikat erstellt wird, werden in diesem Datensatz auch Ereignisse aufgezeichnet, die sich auf dieses Zertifikat beziehen. Der Registrierungssatz enthält also alle Ereignisse, die während der Gültigkeitsdauer der Anforderung und des zugehörigen Zertifikats aufgetreten sind.

Datensatzattribute

Die Attribute eines Datensatzes in der Registrierungsdatenbank sind Variablen, die zur Beschreibung der Registrierungsanforderung dienen. Bei ausgeführten Anforderungen beschreiben die Variablen außerdem das genehmigte Zertifikat. Andere Attribute definieren Verarbeitungsvariablen, die Ihr Unternehmen bei der Implementierung der Unternehmensregeln unterstützen. Einige der Attribute und der zugehörigen Werte können vom Registrator über RA Desktop angezeigt werden.

Zertifizierung

Als Zertifizierung bezeichnet man die Erstellung eines digitalen Zertifikates für eine Entität oder eine Person. Unter Tivoli PKI wird die Zertifizierung nur nach der Auswertung und Genehmigung einer Registrierungsanforderung ausgeführt. Nach der Registrierung werden vom Zertifikatsaussteller (CA) die angeforderten Zertifikate ausgestellt. Bei Tivoli PKI stimmt der Zertifikatstyp des ausgestellten Zertifikats mit den Unternehmensregeln des jeweiligen Unternehmens überein.

Zertifikatsaussteller

Unter Tivoli PKI ist der CA als Server-Programm implementiert, das für die Ausstellung digitaler Zertifikate in Übereinstimmung mit den Regeln eines Unternehmens verantwortlich ist.

Tivoli PKI unterstützt die gegenseitige Zertifizierung, bei der CAs, die gegenseitig abgesichert sind, vereinbarungsgemäß die Zertifikate des jeweiligen Partner-CAs als Authentifizierung akzeptieren. Tivoli PKI unterstützt außerdem eine bestimmte CA-Hierarchie. CAs identifizieren andere CAs dann als zuverlässig, wenn sie sich innerhalb der Hierarchie über ihnen befinden. In diesem Fall akzeptieren sie die Zertifikate dieser CAs als Authentifizierungsbeleg.

Zertifikatswiderrufslisten (CRL)

Die Registrierungsstelle von Tivoli PKI veröffentlicht in regelmäßigen Zeitabständen eine Zertifikatswiderrufsliste (CRL = Certificate Revocation List). Diese CRLs enthalten eine Liste der Zertifikate, deren Gültigkeitszeitraum abgelaufen ist. Werden diese Zertifikate vorgelegt, können die zugehörigen Eigner nicht authentifiziert werden.

Alle CAs, RAs und Anwendungen können auf diese Liste zugreifen, um festzustellen, ob ein bestimmtes Zertifikat widerrufen wurde. Auf diese Weise kann die Registrierungsstelle von Tivoli PKI beim Zugriff auf die gesicherten Anwendungen Ihres Unternehmens die Sicherheit aller verfügbaren Ressourcen gewährleisten.

Verzeichnisse (Directory)

Das Verzeichnis, das von Tivoli PKI zum Speichern von Zertifikaten verwendet wird, ist das IBM Directory. Dieses Verzeichnis wurde in Ihrem Unternehmen möglicherweise für die ausschließliche Verwendung unter Tivoli PKI konfiguriert. Alternativ hierzu kann es sich auch um ein Verzeichnis handeln, das zuvor installiert und für andere Anwendungen eingesetzt wurde.

Als Protokoll für den Zugriff auf das Directory wird von Tivoli PKI das Lightweight Direct Access Protocol (LDAP) verwendet.

Registrierte Namen

Der registrierte Name (DN = Distinguished Name) ist Bestandteil des Directory-Eintrags für ein digitales Zertifikat. Er dient zur eindeutigen Identifizierung der Position des Eintrags in der hierarchischen Struktur des Directory.

Zertifikate

Bei einem Zertifikat handelt es sich um einen digitalen Identitätsnachweis, der von einem CA unterschrieben wird, der für die Identität des Zertifikatseigners bürgt. Der Eigner kann das Zertifikat bei der Kommunikation mit anderen Benutzern oder zur Anforderung des Zugriffs auf eine gesicherte Anwendung als Authentifizierung verwenden. Unter Tivoli PKI müssen auch Server, Anwendungen und Einheiten (z. B. Drucker oder Smart Cards) über Zertifikate verfügen, um sie gegenüber Benutzern und untereinander zu authentifizieren.

Tivoli PKI unterstützt X.509v3-Zertifikate der folgenden Kategorien:

- Browser-Zertifikate
- Server-Zertifikate
- Einheitenzertifikate
- Zertifikate für den Zugriff auf PKIX-kompatible Anwendungen
- Zertifikate zur gegenseitigen Zertifizierung für CAs

Tivoli PKI unterstützt außerdem die folgenden Protokolle:

- SSL
- S/MIME
- IPSec
- PKIX CMP

Eine Standardinstallation von Tivoli PKI bietet eine Vielzahl von Zertifikatstypen, die auf diesen Kategorien und Protokollen basieren. Antragsteller für die Registrierung können Zertifikate anfordern, die auf ihre individuellen Vorgaben zugeschnitten sind. Im Abschnitt „Gelieferte Zertifikatstypen” auf Seite 49 werden die einzelnen Zertifikatstypen beschrieben.

Browserzertifikate

Bei einem Browser-Zertifikat handelt es sich um einen digitalen Identitätsnachweis, der normalerweise von Ihrem Web-Browser in einer verschlüsselten Datei gespeichert wird. Bestimmte Anwendungen erlauben die Speicherung der Schlüssel auf einer Smart Card oder einem anderen Speichermedium. In einem Tivoli PKI-System können Sie ein Browser-Zerti-

fikat direkt über Ihren Web-Browser anfordern. Später können Sie bei Bedarf auf die Web-Seite für die Registrierung zurückkehren und das Zertifikat erneuern oder widerrufen.

CA-Zertifikate

Alle Browser, Server, Einheiten oder Anwendungen, die über ein Zertifikat zur Vorlage beim Tivoli PKI-Server verfügen, müssen außerdem ein kompatibles CA-Zertifikat besitzen. Dieses Zertifikat wird zur Authentifizierung der Kommunikation zwischen Servern benötigt, die über vom Tivoli PKI-CA ausgestellte Zertifikate verfügen.

Sie müssen in Ihrem Browser ein Tivoli PKI-CA-Zertifikat haben, um die gesicherten Registrierungsservices von Tivoli PKI einsetzen zu können. Dieses CA-Zertifikat kann beim ersten Besuch der Registrierungs-Web-Seiten von Tivoli PKI abgerufen werden. Anschließend können Sie bei jeder Anforderung eines Zertifikates bei den Registrierungsservices auch das zugehörige, kompatible CA-Zertifikat herunterladen.

Beispiel: Wenn Sie ein SSL-Browser-Zertifikat mit einem Gültigkeitszeitraum von 2 Jahren anfordern, können Sie ein CA-Zertifikat empfangen, das mit diesem Zertifikat kompatibel ist.

Anmerkung: Frühere Releases von Netscape konnten ein Site-Zertifikat akzeptieren, das von einem Tivoli PKI-Server vorgelegt wurde. Dieses Zertifikat war sowohl für die server-authentifizierte als auch für die client-authentifizierte Kommunikation mit diesem Server akzeptabel. Beim neuesten Netscape-Release wird jedoch ein CA-Zertifikat für client-authentifizierte Sitzungen benötigt.

Server- oder Einheitenzertifikate

Wenn dies zu Ihren Aufgabengebieten gehört, können Sie Zertifikate für Server oder Einheiten anfordern. Verwenden Sie hierzu das Registrierungsformular, das über Ihren Web-Browser zur Verfügung steht.

Der Server bzw. die Einheit, für den bzw. die Sie ein Zertifikat anfordern, muss das PKCS #10-Anforderungsformat verwenden.

Zertifikatserweiterungen

Zertifikatserweiterungen sind optionale Elemente, die im Format eines X.509v3-Zertifikats definiert sind. Durch die Erweiterungen ist es möglich, zusätzliche Felder in das Zertifikat aufzunehmen. Tivoli PKI stellt eine Gruppe mit Zertifikatserweiterungen zur Verfügung, mit deren Hilfe Sie die Zertifikate, die von Ihrem Unternehmen ausgestellt werden, anpassen können. Diese zusätzlichen Felder werden als *Unternehmensprozessvariablen* bezeichnet.

Wenn Sie einen Datensatz in RA Desktop anzeigen, können Sie diese Felder sehen, wenn die Verarbeitungsattribute ausgegeben werden. In bestimmten Fällen können Sie die zugehörigen Werte aktualisieren.

Gültigkeitsdauer von Zertifikaten

Bei der Anforderung eines Zertifikates starten Sie einen Gültigkeitszeitraum, der den gesamten Verarbeitungszeitraum dieses Identitätsnachweises umfasst. Dieser Gültigkeitszeitraum endet, wenn das Zertifikat widerrufen oder sein Ablaufdatum erreicht wird.

Als RA-Administrator können Sie Zertifikate auch aussetzen und reaktivieren.

Wird ein Zertifikat erneuert, wird in der Registrierungsdatenbank ein neuer Datensatz erstellt.

Aussetzen und Wiederaufnehmen von Zertifikaten

Unter bestimmten Umständen wird möglicherweise die Aussetzung eines Zertifikats angefordert. Dies kann beispielsweise dann der Fall sein, wenn der Eigner eines Zertifikats vermutet, dass die Sicherheit seines Zertifikats kompromittiert ist. Ebenso kann im Anschluss an eine entsprechende Untersuchung angefordert werden, das ausgesetzte Zertifikat zu reaktivieren. Diese Aufgaben werden über RA Desktop ausgeführt. Will ein Benutzer, dass sein Zertifikat ausgesetzt wird, kann er eine entsprechende Anforderung ausgeben. Soll das betreffende Zertifikat reaktiviert werden, muss die Reaktivierung per E-Mail oder auf anderem Kommunikationsweg angefordert werden. Mitteilungen an den Benutzer, der die Anforderung stellt, sind auf dieselbe Weise zu handhaben.

Jedes Zertifikat verfügt über eine Karenzzeit, die vom Zertifikatstyp abhängt und im Zertifikatsprofil definiert ist. Als RA-Administrator können Sie die Standardkarenzzeit ändern. Der Wert Null steht für 'unendlich' und bedeutet, dass das Zertifikat jederzeit wieder aufgenommen werden kann, sofern es noch nicht abgelaufen ist. Nach Ablauf der Karenzzeit kann ein Zertifikat nicht mehr reaktiviert werden.

Über den Parameter 'max_times_suspended' in der Datei 'certificate_profiles.cfg' kann angegeben werden, wie oft ein Zertifikat ausgesetzt werden darf. Der Standardwert für diesen Parameter ist Null, d. h., es gibt keine Begrenzung. Wird der Standardwert geändert, gilt Folgendes: Wurde ein bestimmtes Zertifikat zuvor schon einmal ausgesetzt, kann über RA Desktop angezeigt werden, wie oft das betreffende Zertifikat bereits ausgesetzt wurde. Nach Erreichen des Grenzwerts wird das Zertifikat widerrufen. Die maximal zulässige Anzahl der Aussetzungen kann ebenfalls angezeigt werden. Das Handbuch *Tivoli PKI Anpassung* enthält weitere Informationen darüber, wie Zertifikatsprofile geändert werden.

Erneuerbarkeit

Die Erneuerbarkeit eines Zertifikats stellt eines der Merkmale dar, die von Ihnen über RA Desktop geändert werden können:

- Wird ein Zertifikat als erneuerbar definiert, kann der Eigner ein neues Zertifikat beantragen, solange das alte noch gültig ist. Besitzt ein Benutzer ein erneuerbares Zertifikat, vereinfacht sich hierdurch der Registrierungsprozess und der erforderliche Aufwand.
- Wird ein Zertifikat als nicht erneuerbar definiert, muss sein Eigner das Ablaufdatum abwarten und anschließend eine neue Registrierung beantragen, wenn das Zertifikat weiterhin benötigt wird. Bei der Registrierung müssen alle Informationen in derselben Weise erneut bereitgestellt werden wie bei einer Erstregistrierung.

Bestimmte Benutzer können eigene Erneuerungsanforderungen übergeben:

- Benutzer mit erneuerbaren Browser-Zertifikaten können die Erneuerung auf der Registrierungs-Web-Seite anfordern.
- Benutzer mit erneuerbaren Zertifikaten für den Zugriff auf PKIX-kompatible Anwendungen können die Erneuerung mit Hilfe der Client-Anwendung von Tivoli PKI anfordern.

Sicherung und Wiederherstellung von Zertifikatsschlüsseln

Endbenutzer können das Erstellen und Wiederherstellen einer Sicherungsdatei anfordern, die Informationen zu ihrem Zertifikat und privaten Schlüssel enthält. Dies ist dann nützlich, wenn der Schlüsselinhaber seinen Schlüssel vergisst oder dieser verloren geht. Die Sicherungsdatei wird entweder über einen Browser oder über die Client-Anwendung im PKCS #12-Format erstellt und in der Systemdatenbank 'krbdb' für die Wiederherstellung von Schlüsseln gespeichert.

Der Registrator hat die Möglichkeit, diese Anforderungen über RA Desktop zu prüfen und die Wiederherstellung der Sicherungsdatei gegebenenfalls zu autorisieren. Aus der Datenbank 'krbdb' kann der Registrator das entschlüsselte Kennwort, die fortlaufende Nummer des Zertifikats und die Informationen zum Aussteller anzeigen. Wird die Anforderung genehmigt, wird die Sicherungsdatei dem Benutzer zum Herunterladen zur Verfügung gestellt. Genehmigungen zum Wiederherstellen von Schlüsseln werden über RA Desktop verwaltet.

Publizieren von Zertifikaten

Bei Tivoli PKI werden Zertifikate nach dem Ausstellen automatisch publiziert. Schlägt diese Publizierung fehl, kann der Registrator die betreffenden Zertifikate mit Hilfe von RA Desktop erneut für das Verzeichnis (Directory) publizieren.

Verwaltung

Bevor Sie Ihre Aufgaben als Registrator ausführen können, müssen Sie ein Zertifikat für den Web-Browser anfordern und erhalten, den Sie für die Verwendung von RA Desktop einsetzen möchten. Nach dem Empfang des Browser-Zertifikats müssen Sie dieses immer dann vorlegen, wenn Sie auf RA Desktop zugreifen möchten. Um Operationen mit Registrierungssätzen oder Anforderungen auszuführen oder diese über RA Desktop anzuzeigen, müssen Sie außerdem über die benötigten Dateiberechtigungen verfügen.

Die Abschnitte in diesem Kapitel enthalten Informationen zur Verwendung und Verwaltung von Zertifikaten.

Zugriffssteuerung

Eine Zugriffssteuerungsliste (ACL = Access Control List) dient zur Authentifizierung und Berechtigung interner Tivoli PKI-Benutzer, -Einheiten und -Softwarekomponenten. Beispiel: Das RA Desktop-Unterstützungs-Servlet verwendet die ACL zur Authentifizierung und Berechtigung von Registratoren, bevor ihnen der Zugriff auf RA Desktop gewährt wird.

Authentifizierung und Berechtigung

Durch die Authentifizierung wird die Identität eines Benutzers überprüft, durch die entsprechende Berechtigung wird es hingegen für einen Benutzer möglich, bestimmte Operationen auszuführen. Tivoli PKI ermöglicht Ihrem Unternehmen, beide Nachweise zwingend anzufordern, bevor einem bestimmten Benutzer der Zugriff auf gesicherte Anwendungen gewährt wird. Andererseits kann für Zertifikatseigner durch diesen Sicherungsmechanismus gewährleistet werden, dass die benutzten Anwendungen auch tatsächlich sicher sind.

Parallele Verwaltung

Tivoli PKI stellt eine einzige Registrierungsdomäne zur Verfügung, es können jedoch mehrere Registratoren parallel in dieser Domäne arbeiten. Das Design des RA Desktop-Servlets und die RA verhindern, dass ein Datensatz aktualisiert werden kann, solange ein anderer Benutzer auf diesen zugreift. Allerdings ist es möglich, dass mehrere Administratoren gleichzeitig einen bestimmten Datensatz anzeigen.

Servlet zur Unterstützung von RA Desktop

Das RA Desktop-Unterstützungs-Servlet ist eine Tivoli PKI-Anwendung, die die Services von RA Desktop für Registratoren zur Verfügung stellt. Das Servlet gibt Informationen zurück, wenn ein Registrator eine Abfrage ausführt, und aktualisiert darüber hinaus Datensätze, deren Änderung ein Registrator genehmigt hat.

Anforderungsprofile

Tivoli PKI stellt eine Standardgruppe mit Anforderungsprofilen zur Verfügung, die von Ihrem Unternehmen zur Vereinfachung der Registrierung und Zertifizierung verwendet werden können. Ein Anforderungsprofil steuert die Attribute und die Verarbeitung von Registrierungsanforderungen. Jedes Anforderungsprofil umfasst eine Schablone für ein Zertifikat. Es gibt verschiedene Anforderungsprofile für die unterstützten Zertifikatskategorien.

Als Name des Anforderungsprofils eines Elements wird eines der Attribute verwendet. Falls erforderlich, können Sie bei der Genehmigung der Registrierungsanforderung ein anderes Anforderungsprofil angeben.

Möglicherweise wird ein bestimmter Anforderungsprofilname bei den Attributen für Anforderungen und ein anderer bei den Basisattributen aufgelistet. Das bedeutet, dass ein Registrator oder ein RA-Prozess zu einem bestimmten Zeitpunkt das Anforderungsprofil überschrieben hat. Das Profil in den Attributen für die Anforderung wurde zusammen mit anderen Attributen der Registrierungsanforderung temporär inaktiviert. Das Profil in den Basisattributen ist das aktuelle Anforderungsprofil.

5

Referenzinformationen

Die Abschnitte in diesem Kapitel enthalten Feldbeschreibungen, gültige Feldwerte und die Bedeutung von Attributen, die in RA Desktop angezeigt werden. Die Abschnitte sind so organisiert, dass Ihnen die Informationen in RA Desktop dort zur Verfügung stehen, wo sie benötigt werden.

Registerkarte 'Abfrage'

Auf der Registerkarte **Abfrage** können Sie eine Abfrage vorbereiten, mit der Informationen zu Zertifikaten, zur Wiederherstellung von Schlüsseln oder zu Registrierungsanforderungen abgerufen werden können.

Die Registerkarte verfügt über folgende Elemente:

- Felder zum Vorbereiten der Abfrage.
- Einen Knopf **Abfrage übergeben** zum Ausführen der Abfrage.
- Hilfe für Ihre Aufgabe:
  - Einen Statusbereich unten auf der Registerkarte. Hier werden während der Verarbeitung feldspezifische Hilfetexte, Tivoli PKI-Nachrichten und ein Statusbalken angezeigt.
  - Einen Knopf **Hilfe** für die Registerkarte.

Wenn die Ergebnisse der Abfrage vorliegen, zeigt RA Desktop automatisch die Registerkarte **Ergebnisse** an.

Abfragefelder

Verwenden Sie alle Felder, die zur Vorbereitung Ihrer Abfrage erforderlich sind. Bestimmte Felder sind nicht verfügbar, wenn sie sich mit anderen, von Ihnen ausgewählten Feldern gegenseitig ausschließen:

- Klicken Sie unter **Abfrageart** auf eine der folgenden Optionen:
  - **Anhand von Anforderungsstatus, Name und Aktualisierungsdatum**, wenn Sie Datensätze von Registrierungsanforderungen und Zertifikaten auf der Basis ihres Status abrufen möchten.
  - **Anhand von Erneuerbarkeit und Ablaufdatum**, wenn Sie Datensätze von Zertifikaten abrufen möchten, für die Informationen zur Erneuerbarkeit und zum Ablaufdatum benötigt werden.
  - **Anhand von Wiederherstellungsstatus, Name und Aktualisierungsdatum**, wenn Sie Datensätze von Anforderungen zur Wiederherstellung von Zertifikatsschlüsseln abrufen möchten.

- Wenn Sie unter **Abfrageart** die Option **Anhand von Anforderungsstatus, Name und Aktualisierungsdatum** ausgewählt haben, können Sie die Abfrage bei Bedarf mit Hilfe der folgenden Felder weiter differenzieren:
  - Verwenden Sie die Liste unter **Anforderungsstatus** zum Abrufen von Elementen mit allen Statusangaben oder nur zum Abrufen von Elementen mit einem bestimmten Status. Wählen Sie aus der Liste einen der folgenden Werte für den Anforderungsstatus aus. Die Standardauswahl lautet **Anstehend**.

    Alle Mit dieser Option werden alle Registrierungsanforderungen oder Schlüsselwiederherstellungsanforderungen unabhängig vom Status abgerufen.

    Empfangen
    Mit dieser Option werden neu empfangene Registrierungsanforderungen oder Schlüsselwiederherstellungsanforderungen abgerufen.

    Anstehend
    Mit dieser Option werden Anforderungen abgerufen, die noch nicht genehmigt oder zurückgewiesen wurden. Bestimmte anstehende Anforderungen sind neu. Hier müssen Sie eine Entscheidung treffen. Bei anderen müssen Sie auf das Eintreffen weiterer Informationen warten, bevor sie weiterbearbeitet werden können. Dies ist der Standardwert.

    Genehmigt
    Mit dieser Option werden Anforderungen abgerufen, die von einer RA oder einem Registrator genehmigt wurden. Der Status der zugehörigen Zertifikate kann variieren.

    Nicht genehmigt
    Mit dieser Option werden Anforderungen abgerufen, die von einer RA oder einem Registrator nicht genehmigt wurden.

    Abgeschlossen
    Mit dieser Option werden Anforderungen abgerufen, die von einer RA oder einem Registrator entweder genehmigt oder nicht genehmigt wurden. Bei genehmigten Anforderungen mit diesem Status wurde das Zertifikat an den Benutzer übergeben.

  - Verwenden Sie die folgenden Felder ausschließlich zum Abrufen von Datensätzen für Anforderungen oder Zertifikate, die einem bestimmten Namen zugeordnet sind:
    - Geben Sie unter **Nachname** den Nach- oder Familiennamen ein. Sie können auch nur die ersten Buchstaben eines Namens eingeben, um alle Namen abzurufen, die mit dieser Buchstabenfolge beginnen. Beispiel: Wenn Sie die Buchstabenfolge ″Smi*″ eingeben, werden alle Datensätze mit den Namen ″Smith″, ″Smithers″, ″Smiley″ sowie andere Nachnamen abgerufen, die mit der Buchstabenfolge ″Smi″ beginnen.
    - Geben Sie unter **Vorname** den Vornamen ein. Sie können auch nur die ersten Buchstaben eines Namens eingeben, um alle Namen abzurufen, die mit dieser Buchstabenfolge beginnen. Beispiel: Wenn Sie die Buchstabenfolge ″Joh*″ eingeben, werden alle Datensätze mit den Vornamen ″Johanna″, ″John″, ″Johan″ sowie andere Vornamen abgerufen, die mit der Buchstabenfolge ″Joh″ beginnen.
  - Verwenden Sie die Option **Datumsbereiche für die letzte Aktualisierung**, wenn Sie nur die Elemente abrufen möchten, deren letzte Aktualisierung in einem bestimmten Zeitraum durchgeführt wurde. Geben Sie einen Datumsbereich an.

– Einen Standardwert für das Datum gibt es nicht.

– Wenn in keinem der Felder ein Datum angegeben wird, werden alle Datensätze abgerufen, die mit den restlichen Abfragekriterien übereinstimmen.

Um ein Datum anzugeben, klicken Sie auf den Kalender, um diesen zu öffnen, und anschließend auf das gewünschte Datum. Wenn Sie das Datum eingeben, verwenden Sie beim Ausfüllen des Textfensters dasselbe Format, das auch im Kalender benutzt wird.

Von Das früheste Datum innerhalb des Bereichs.

Wenn Sie hier keinen Wert angeben, werden mit der Abfrage alle Datensätze abgerufen, die an dem oder vor dem Datum aktualisiert wurden, das im Feld **Bis** angegeben wird.

Bis Das neueste Datum innerhalb des Bereichs.

Wenn Sie in diesem Feld keinen Wert angeben, werden mit der Abfrage alle Datensätze abgerufen, die an dem oder nach dem Datum aktualisiert wurden, das im Feld **Von** angegeben wird.

- Wenn Sie unter **Abfrageart** die Option **Anhand von Wiederherstellungsstatus, Name und Aktualisierungsdatum** ausgewählt haben, können Sie die Abfrage bei Bedarf mit Hilfe der folgenden Felder weiter differenzieren:

  - Verwenden Sie die Liste unter **Schlüsselwiederherstellungsstatus** zum Abrufen von Elementen mit allen Statusangaben oder nur zum Abrufen von Elementen mit einem bestimmten Status. Wählen Sie aus der Liste einen der folgenden Werte für den Anforderungsstatus aus. Die Standardauswahl lautet **Alle**.

    Alle Mit dieser Option werden alle Registrierungsanforderungen oder Schlüsselwiederherstellungsanforderungen unabhängig vom Status abgerufen.

    Empfangen
    Mit dieser Option werden neu empfangene Registrierungsanforderungen oder Schlüsselwiederherstellungsanforderungen abgerufen.

    Anstehend
    Mit dieser Option werden Anforderungen abgerufen, die noch nicht genehmigt oder zurückgewiesen wurden. Bestimmte anstehende Anforderungen sind neu. Hier müssen Sie eine Entscheidung treffen. Bei anderen müssen Sie auf das Eintreffen weiterer Informationen warten, bevor sie weiterbearbeitet werden können. Dies ist der Standardwert.

    Genehmigt
    Mit dieser Option werden Anforderungen abgerufen, die von einer RA oder einem Registrator genehmigt wurden. Der Status der zugehörigen Zertifikate kann variieren.

    Nicht genehmigt
    Mit dieser Option werden Anforderungen abgerufen, die von einer RA oder einem Registrator nicht genehmigt wurden.

    Abgeschlossen
    Mit dieser Option werden Anforderungen abgerufen, die von einer RA oder einem Registrator entweder genehmigt oder nicht genehmigt wurden. Bei genehmigten Anforderungen mit diesem Status wurde das Zertifikat an den Benutzer übergeben.

Nicht versucht
Mit dieser Option werden Registrierungsanforderungen abgerufen, für die entweder keine Schlüsselsicherungs- oder keine Schlüsselwiederherstellungsanforderung versucht wurde.

- Verwenden Sie die folgenden Felder ausschließlich zum Abrufen von Datensätzen für Anforderungen oder Zertifikate, die einem bestimmten Namen zugeordnet sind:
  - Geben Sie unter **Nachname** den Nach- oder Familiennamen ein. Sie können auch nur die ersten Buchstaben eines Namens eingeben, um alle Namen abzurufen, die mit dieser Buchstabenfolge beginnen. Beispiel: Wenn Sie die Buchstabenfolge ″Smi*″ eingeben, werden alle Datensätze mit den Namen ″Smith″, ″Smithers″, ″Smiley″ sowie andere Nachnamen abgerufen, die mit der Buchstabenfolge ″Smi″ beginnen.
  - Geben Sie unter **Vorname** den Vornamen ein. Sie können auch nur die ersten Buchstaben eines Namens eingeben, um alle Namen abzurufen, die mit dieser Buchstabenfolge beginnen. Beispiel: Wenn Sie die Buchstabenfolge ″Joh*″ eingeben, werden alle Datensätze mit den Vornamen ″Johanna″, ″John″, ″Johan″ sowie andere Vornamen abgerufen, die mit der Buchstabenfolge ″Joh″ beginnen.
- Verwenden Sie die Option **Datumsbereiche für die letzte Aktualisierung**, wenn Sie nur die Elemente abrufen möchten, deren letzte Aktualisierung in einem bestimmten Zeitraum durchgeführt wurde. Geben Sie einen Datumsbereich an.
  - Einen Standardwert für das Datum gibt es nicht.
  - Wenn in keinem der Felder ein Datum angegeben wird, werden alle Datensätze abgerufen, die mit den restlichen Abfragekriterien übereinstimmen.

  Um ein Datum anzugeben, klicken Sie auf den Kalender, um diesen zu öffnen, und anschließend auf das gewünschte Datum. Wenn Sie das Datum eingeben, verwenden Sie beim Ausfüllen des Textfensters dasselbe Format, das auch im Kalender benutzt wird.

  Von Das früheste Datum innerhalb des Bereichs.

  Wenn Sie hier keinen Wert angeben, werden mit der Abfrage alle Datensätze abgerufen, die an dem oder vor dem Datum aktualisiert wurden, das im Feld **Bis** angegeben wird.

  Bis Das neueste Datum innerhalb des Bereichs.

  Wenn Sie in diesem Feld keinen Wert angeben, werden mit der Abfrage alle Datensätze abgerufen, die an dem oder nach dem Datum aktualisiert wurden, das im Feld **Von** angegeben wird.

- Wenn Sie unter **Abfrageart** die Option **Anhand von Erneuerbarkeit und Ablaufdatum** ausgewählt haben, können Sie die Abfrage bei Bedarf mit Hilfe der folgenden Felder weiter differenzieren:
  - Verwenden Sie die Liste unter **Erneuerbarkeit**, um eine Abfrage auf dem Kriterium der Erneuerbarkeit eines Zertifikates zu basieren. Wählen Sie aus der Liste einen der folgenden Werte aus:

    Erneuerbar
    Das Zertifikat kann erneuert werden, wenn es noch nicht ausgelaufen ist.

Nicht erneuerbar
Das Zertifikat kann nicht erneuert werden.

- Verwenden Sie die Option **Bereich der Ablaufdaten**, um nur solche Elemente abzurufen, die während eines bestimmten Zeitraums ablaufen. Geben Sie einen Datumsbereich an.
  - Einen Standardwert gibt es nicht.
  - Wenn in keinem der Felder ein Datum angegeben wird, werden alle Datensätze abgerufen, die mit den restlichen Abfragekriterien übereinstimmen.

  Um ein Datum anzugeben, klicken Sie auf den Kalender, um diesen zu öffnen, und anschließend auf das gewünschte Datum. Wenn Sie das Datum eingeben, verwenden Sie beim Ausfüllen des Textfensters dasselbe Format, das auch im Kalender benutzt wird.

  Von Das früheste Ablaufdatum.

  Wenn Sie hier keinen Wert angeben, werden mit der Abfrage alle Datensätze abgerufen, die an dem oder vor dem Datum auslaufen, das im Feld **Bis** angegeben wird.

  Bis Das neueste Ablaufdatum.

  Wenn Sie hier keinen Wert angeben, werden mit der Abfrage alle Datensätze abgerufen, die an dem oder nach dem Datum auslaufen, das im Feld **Von** angegeben wird.

- Verwenden Sie eines oder beide der folgenden Felder, um die Verarbeitung und Anzeige Ihrer Abfrage zu steuern:

  Anzahl der abzurufenden Datensätze
  Die maximale Anzahl von abzurufenden Datensätzen unabhängig von der Anzahl der Datensätze, die tatsächlich mit den Abfragekriterien übereinstimmen. Wählen Sie einen der folgenden Werte aus:
  - 50
  - 100
  - 150
  - 250 (Standardwert)
  - Unbegrenzt (zum Abrufen aller Datensätze, die mit den Abfragekriterien übereinstimmen)

  Sätze pro Seite
  Die Anzahl der Datensätze, die auf den einzelnen Seiten der Registerkarte **Ergebnisse** angezeigt werden sollen. Sie können in diesen Seiten blättern, um die benötigten Datensätze in den Ergebnisdaten Ihrer Abfrage zu suchen. Wählen Sie entweder einen der folgenden Werte aus oder überschreiben Sie den angezeigten Standardwert mit einer numerischen Angabe.
  - 10
  - 15 (Standardwert)
  - 20
  - 25

Vordefinierte Abfragen

Die einzige vordefinierte Abfrage ist die Standardabfrage, mit der alle anstehenden Anforderungen abgerufen werden.

Anzahl der abzurufenden Datensätze - Optionen

Auf der Registerkarte **Abfrage** stehen die folgenden Optionen zum Definieren der **Anzahl der abzurufenden Datensätze** zur Verfügung:

- 50
- 100
- 150
- 250 (Standardwert)
- Unbegrenzt (zum Abrufen aller Datensätze, die mit den Abfragekriterien übereinstimmen)

Diese Optionen haben Auswirkungen auf die Anzahl der Datensätze in den Abfrageergebnissen auf der Registerkarte **Ergebnisse**.

Sätze pro Seite - Optionen

Auf der Registerkarte **Abfrage** stehen die folgenden Optionen zum Definieren der **Sätze pro Seite** zur Verfügung:

- 10
- 15 (Standardwert)
- 20
- 25
- Alle numerischen Werte, die anstelle des angezeigten Standardwertes eingegeben werden

Diese Optionen haben Auswirkungen auf die Anzeige der Abfrageergebnisse auf der Registerkarte **Ergebnisse**.

Registerkarte 'Ergebnisse'

Auf der Registerkarte **Ergebnisse** werden die Ergebnisse der Ausführung einer Abfrage angezeigt. Die Registerkarte verfügt über folgende Elemente:

- Eine Tabelle mit den Ergebnissen der Abfrage.
  - Jede Zeile enthält hierbei den Datensatz eines Elementes, das mit den Abfragekriterien übereinstimmt.
  - Sie können die Zeilen auf der Basis der Werte in einer bestimmten Zeile sortieren.
  - Sie können für die Spalten eine Größenanpassung vornehmen, um ihre Breite zu ändern.
  - Sie können in den Ergebnisdaten blättern, wenn eine Tabellenseite die Länge der Anzeige überschreitet.
  - Wenn die Ergebnisdaten auf mehreren Seiten angezeigt werden, können Sie auf **Nächste Seite** und **Vorhergehende Seite** klicken, um alle Daten zu sehen.

    Anmerkung: Bei der Anforderung der nächsten oder vorhergehenden Seite kann es eventuell zu Verzögerungen kommen. Die Seiten werden bei Bedarf vom Server abgerufen. Lokal steht immer nur die aktuelle Seite zur Verfügung.
- Felder zum Definieren des Gültigkeitszeitraums eines Zertifikates, falls erforderlich.
- Ein Feld, in dem bei Bedarf ein anderes Anforderungsprofil für eine Anforderung angegeben werden kann, die momentan genehmigt wird.

- Eine Auswahlliste mit den Aktionen, die für die Verarbeitung von einem oder mehreren ausgewählten Elementen zur Verfügung stehen. Wenn als Aktion ″Widerrufen″ ausgewählt wurde, wird außerdem eine Auswahlliste für die Gründe des Widerrufs angezeigt.
- Ein Feld für Kommentare, in dem ein Kommentar zu der ausgeführten Aktion eingegeben werden kann.
- Einen Knopf **Details anzeigen** zur detaillierteren Anzeige eines Datensatzes. Wenn Sie auf diesen Knopf klicken, zeigt RA Desktop die Registerkarte **Details** an.
- Einen Knopf **Aktion übergeben** zum Ausführen der ausgewählten Aktion.
- Hilfe für Ihre Aufgabe:
  - Einen Statusbereich unten auf der Registerkarte. Hier werden während der Verarbeitung feldspezifische Hilfetexte, Tivoli PKI-Nachrichten und ein Statusbalken angezeigt.
  - Einen Knopf **Hilfe** für die Registerkarte.

Wenn Sie auf die Registerkarte **Abfrage** klicken, wird diese erneut aufgerufen, sodass Sie die Abfrage differenzieren oder eine weitere Abfrage vorbereiten können.

Verwaltungsaktionen

Die einzigen Aktionen, die für Sie zur Verfügung stehen, sind die Berechtigungen für das Arbeiten mit Datensätzen. Die folgenden Optionen werden angezeigt:

Genehmigen
Mit dieser Option wird die Anforderung genehmigt, damit dem Antragsteller das angeforderte Zertifikat ausgestellt werden kann.

Als ″anstehend″ behalten
Mit dieser Option wird die Entscheidung verzögert. Verwenden Sie diese Option, wenn Sie zur Bearbeitung des Antrags noch externe Informationen benötigen oder lediglich einen Kommentar an den Datensatz anfügen möchten.

Zurückweisen
Mit dieser Option wird die Anforderung abgewiesen.

Zertifikat widerrufen
Mit dieser Option wird die Gültigkeit eines Zertifikates beendet.

Zertifikat aussetzen
Mit dieser Option wird die Gültigkeit eines Zertifikats vorübergehend ausgesetzt.

Zertifikat wieder aufnehmen
Mit dieser Option wird ein ausgesetztes Zertifikat reaktiviert.

Anforderung als ’Erneuerbar’ definieren
Mit dieser Option wird der Status eines nicht erneuerbaren Zertifikates in ″erneuerbar″ geändert.

Anforderung als ’Nicht erneuerbar’ definieren
Mit dieser Option wird der Status eines erneuerbaren Zertifikates in ″nicht erneuerbar″ geändert.

Zertifikat publizieren
Mit dieser Option wird ein Zertifikat für das Verzeichnis (Directory) publiziert.

Schlüsselwiederherstellung genehmigen
Mit dieser Option wird eine Schlüsselwiederherstellungsanforderung genehmigt, damit dem Antragsteller die wiederhergestellte PKCS #12-Datei zur Verfügung gestellt werden kann.

Schlüsselwiederherstellung zurückweisen
Mit dieser Option wird eine Schlüsselwiederherstellungsanforderung abgewiesen.

Keine Aktion verfügbar
Diese Option gibt an, dass Sie lediglich über die Berechtigung zum Anzeigen der Datensätze in der Registrierungsdomäne verfügen.

Gründe für das Widerrufen eines Zertifikats

Wenn Sie ein Zertifikat widerrufen, müssen Sie eine entsprechende Begründung auswählen. Im folgenden sind die zulässigen Begründungen aufgeführt, die für den Widerruf eines Zertifikats ausgewählt werden können.

Wenn Sie die Details eines Datensatzes anzeigen und seine Verarbeitungsattribute prüfen, kann im Attribut für die Widerrufbegründung einer der folgenden Werte definiert sein:

Der CA-Schlüssel war beschädigt
Der Schlüssel des Zertifikatsausstellers wurde beschädigt.

Das Zertifikat wurde ersetzt
Der Benutzer verfügt über ein neues Zertifikat und benötigt dieses nicht mehr.

Kein Begründung
Der Benutzer hat den Widerruf ohne Angabe einer Begründung angefordert.

Der ursprüngliche Verwendungszweck ist nicht mehr gültig
Der Zertifikatseigner benötigt das Zertifikat nicht mehr für seine ursprüngliche Verwendung.

Benutzer hat die Zugehörigkeit geändert
Der Benutzer verfügt nicht mehr über die Zugehörigkeit, für die das Zertifikat angefordert wurde.

Der Benutzerschlüssel war beschädigt
Der private Schlüssel des Benutzers wurde beschädigt.

Registerkarte 'Details'

Auf der Registerkarte **Details** können Sie die Details eines Datensatzes anzeigen, der aus der Liste der Datensätze ausgewählt wurde, die mit den Abfragekriterien übereinstimmen. Die Registerkarte verfügt über folgende Elemente:

- Eine Liste zum Auswählen des anzuzeigenden Detailtyps. Die Liste umfasst das Aktionsprotokoll des Elements und verschiedene Gruppen mit Attributen, die zu dem Element gehören. Der Abschnitt „Detailgruppen" auf Seite 50 enthält eine Beschreibung zu diesen Gruppen.
- Eine Tabelle, in der der ausgewählte Detailtyp angezeigt wird:
  - Wenn Sie die Attribute anzeigen, enthält jede Zeile ein Attribut sowie den zugehörigen Wert. Bei der Genehmigung der Registrierungsanforderung können Sie bestimmte Werte aktualisieren.

- Wenn Sie das Aktionsprotokoll anzeigen, steht jede Zeile für eine Aktion, die für das Element ausgeführt wurde.
- Sie können die Zeilen auf der Basis der Werte in einer bestimmten Zeile sortieren.
- Sie können für die Spalten eine Größenanpassung vornehmen, um ihre Breite zu ändern.

- Felder zum Definieren des Gültigkeitszeitraums eines Zertifikates, falls erforderlich.
- Ein Feld, in dem bei Bedarf ein anderes Anforderungsprofil für eine Anforderung angegeben werden kann, die momentan genehmigt wird.
- Eine Auswahlliste mit den Aktionen, die zur Verfügung stehen. Wenn als Aktion **Wiederrufen** ausgewählt wurde, wird außerdem eine Auswahlliste für die Gründe des Widerrufs angezeigt.
- Ein Feld für Kommentare, in dem ein Kommentar zu der ausgeführten Aktion eingegeben werden kann.
- Einen Knopf **Details aktualisieren** zum Aktualisieren der Anzeige.
- Einen Knopf **Aktion übergeben** zum Ausführen der ausgewählten Aktion.
- Hilfe für Ihre Aufgabe:
  - Einen Statusbereich unten auf der Registerkarte. Hier werden während der Verarbeitung feldspezifische Hilfetexte, Tivoli PKI-Nachrichten und ein Statusbalken angezeigt.
  - Einen Knopf **Hilfe** für die Registerkarte.

Wenn Sie auf die Registerkarte **Abfrage** klicken, wird diese erneut aufgerufen, sodass Sie die Abfrage differenzieren oder eine weitere Abfrage vorbereiten können. Wenn Sie auf die Registerkarte **Ergebnisse** klicken, wird diese erneut aufgerufen, sodass Sie die Bearbeitung der Abfrageergebnisse fortsetzen können.

Aktionsprotokoll - Ereignisse

Die Tabelle mit Abfrageergebnissen auf der Registerkarte **Ergebnisse** und die Aktionsprotokolltabelle auf der Registerkarte **Details** verfügen über ähnliche Spalten. Die Spalte für den **Anforderungsstatus** beschreibt RA-Aktionen für die Registrierungsanforderung. Die Spalte für den **Ausführungsstatus** beschreibt den Verarbeitungsstatus der Anforderung.

- Auf der Registerkarte **Ergebnisse** wird in der Tabelle mit Abfrageergebnissen der aktuelle Status für alle in den Abfrageergebnissen enthaltenen Elemente angezeigt.
- Auf der Registerkarte **Details** werden in den Spalten der Aktionsprotokolltabelle alle vorhergehenden Statusangaben sowie der aktuelle Status des angezeigten Elementes aufgeführt.

Attribute von Anforderungen und Zertifikaten

Die folgenden Attribute sind als **Anforderungsattribute** klassifiziert. Bei bestimmten Attributen können die zugehörigen Werte geändert werden.

Ablaufdatum des Identitätsnachweises
Das Datum, an dem die Gültigkeit des Zertifikats abläuft.

Status ″Erneuerbar″ des Identitätsnachweises
Gibt an, ob das Zertifikat erneuert werden kann.

Allgemeine, eindeutige Identitätsnachweis-ID
Die allgemeine, eindeutige Identitätsnachweis-ID (UUID = Universal Unique Identifier) ist ein Primärschlüssel, der generiert wird, um einen Index für den Datenbankeintrag bereitzustellen.

Fehlercode
Ein interner Code zur Kennzeichnung der Art des aufgetretenen Fehlers. Dieses Feld und das Feld **Fehlerursache** beschreiben den gleichen Fehler.

Fehlerursache
Der Prozess oder ein anderes Element von Tivoli PKI, in dem während der Verarbeitung von RA Desktop-Anforderungen ein Fehler aufgetreten ist.

Vorname
Das erste Element im vollständigen Namen eines Antragstellers. Obwohl hier normalerweise der Vorname des Antragstellers angegeben wird, kann der Wert auch den zweiten Vornamen oder dessen Initiale umfassen.

Ausführungsstatus
Der Status der Anforderungsverarbeitung. Dieser Status wird im Aktionsprotokoll angezeigt. Der Abschnitt „Status der Registrierungsanforderungen" auf Seite 51 enthält eine Beschreibung der verschiedenen Statuswerte.

Nachname
Der Nach- oder Familienname des Antragstellers.

Vorhergehende Anforderungs-ID
Eine verschlüsselte Zeichenfolge, die für die ID steht, die für eine vorherige Registrierungsanforderung generiert wurde, wenn das Zertifikat erneuert wurde.

Registrierungsdomäne
Die Registrierungsdomäne, die gesicherte Ressourcen für den Eigner eines Zertifikates bereitstellt.

Anforderungs-ID
Eine verschlüsselte Zeichenfolge, die für die ID steht, die für eine Registrierungsanforderung generiert wurde.

Anforderungsprofilname
Mit dieser Option wird die Verarbeitung der Registrierungsanforderung gesteuert. Dieses Profil enthält eine Schablone für das Zertifikat. Die Werte in diesem Profil überschreiben alle anderen Änderungen, die vorgenommen wurden, wenn sie in Widerspruch zum Profil stehen. Der Abschnitt „Gelieferte Zertifikatstypen" auf Seite 49 enthält eine Beschreibung der Merkmale der Zertifikate, die den einzelnen Anforderungsprofilen zugeordnet sind.

Anmerkung: Wenn Sie die Attribute eines Datensatzes anzeigen, werden möglicherweise zwei Anforderungsprofile aufgelistet. Hierbei ist eines den Attributen für die Anforderung und das andere den Basisattributen zugeordnet. Das bedeutet, dass das Anforderungsprofil zu einem bestimmten Zeitpunkt von einem Registrator überschrieben wurde. Das Profil in den Attributen für die Anforderung wurde zusammen mit anderen Attributen der Registrierungsanforderung temporär inaktiviert. Das Profil in den Basisattributen ist das aktuelle Anforderungsprofil.

Anforderungsstatus
Der Status der Registrierungsanforderung. Dieser Status wird im Aktionsprotokoll

angezeigt. Der Abschnitt „Status der Registrierungsanforderungen” auf Seite 51 enthält eine Beschreibung der verschiedenen Statuswerte.

Anforderungsvariablen
Werte, die der Anforderer während des Registrierungsprozesses angegeben hat.

Sicherungsstatus
Status der Schlüsselsicherungsanforderung

Wiederherstellungsstatus
Status der Schlüsselwiederherstellungsanforderung.

Zertifikatserweiterungen

Erweiterungen werden zu Zertifikaten als Paare aus Namen und zugehörigen Werten (name=value) hinzugefügt und können zu den Attributen gehören, die für ein Zertifikat angezeigt werden. Die folgenden Zertifikatserweiterungen können für Zertifikate von Personen verwendet werden, die mit einer gesicherten Anwendung arbeiten möchten:

- Basiseinschränkungen
- Schlüsselverwendung
- Namenseinschränkungen
- Verwendungszeitraum für private Schlüssel
- Alternativer Betreffname

Gelieferte Zertifikatstypen

Ein Tivoli PKI-System stellt verschiedene Zertifikatstypen für die unterstützten Zertifikatskategorien und -protokolle bereit. Diese unterscheiden sich z. B. in den definierten Gültigkeitszeiträumen. Der Name des Zertifikats gibt Aufschluss darüber, wie lange dieses gültig ist, und informiert über die Primärverwendung des Schlüssels. Beschreibungen zu den verschiedenen Merkmalen enthält das Glossar.

Gegenseitiges CA-Zertifikat
Dieses Zertifikat ermöglicht einem CA, der über dieses verfügt, die Sicherung seiner Zertifikate durch den ausstellenden CA. Das Zertifikat stellt eine digitale Unterschrift bereit und unterstützt die Unbestreitbarkeit.

1 und 2 Jahre - Datenverschlüsselung
Dieses Zertifikat ermöglicht dem Eigner die Verschlüsselung von Daten. Das Zertifikat dient nicht zu anderen Zwecken.

1 und 2 Jahre - E-Mail-Schutz
Dieses Zertifikat ermöglicht dem Eigner die Verwendung des S/MIME-Protokolls (S/MIME = Secure Multi-Purpose Internet Mail Exchange). Dieses Protokoll dient zum Schutz von E-Mails und anderen MIME-Objekten. Es unterstützt die Authentifizierung des Absenders, die Integrität von Nachrichten, die Unbestreitbarkeit des Absenders sowie die Vertraulichkeit und wird normalerweise für Endbenutzer verwendet.

1 und 2 Jahre - IPSec
Dieses Zertifikat hilft bei der Gewährleistung der Integrität und Vertraulichkeit von Daten, die in IP-Paketen über das Internet versendet werden. Ein IPSec-Zertifikat ist eher für Daten als für Benutzer geeignet und wird häufig einem Router zugeordnet.

1 und 2 Jahre - Nur Schlüsselcodierung
Dieses Zertifikat ermöglicht dem Eigner die Verschlüsselung von Schlüsseln. Das Zertifikat dient nicht zu anderen Zwecken.

1 und 2 Jahre - Unbestreitbarkeit
Dieses Zertifikat ermöglicht die Nachrichtenverschlüsselung und das digitale Unterzeichnen. Hierdurch wird verhindert, dass der Absender die Ursprungsadresse oder die Übergabe einer Nachricht bestreiten kann.

1 und 2 Jahre - Nur Unterschrift
Dieses Zertifikat ermöglicht dem Eigner die digitale Unterzeichnung einer Datei. Das Zertifikat dient nicht zu anderen Zwecken.

1 und 2 Jahre - Web-Client-Authentifizierung
Dieses Zertifikat ermöglicht einem Web-Browser die Teilnahme an einer client-authentifizierten SSL-Sitzung. Mit ihm kann der Benutzer des Browsers auf eine bestimmte, gesicherte Web-Site zugreifen. Das Zertifikat stellt eine digitale Unterschrift bereit und unterstützt die Unbestreitbarkeit und die Verschlüsselung von Schlüsseln. Es wird normalerweise für Endbenutzer verwendet.

1 und 2 Jahre - Web-Server-Authentifizierung
Dieses Zertifikat ermöglicht einem Server die Teilnahme an einer server-authentifizierten SSL-Sitzung. Das Zertifikat stellt eine digitale Unterschrift bereit und unterstützt die Verschlüsselung von Schlüsseln.

Antragsteller für die Registrierung oder Personen, die eine Vorabregistrierung für andere Personen durchführen, können einen geeigneten Zertifikatstyp anfordern. Wenn Sie ein **Anforderungsprofil** zuordnen, enthält dieses eine Schablone für einen der verfügbaren Zertifikatstypen.

Anmerkung: Die angezeigte Liste stimmt eventuell nicht genau mit der hier dargestellten Liste überein. Ihr Unternehmen hat möglicherweise die Namen oder sogar die angebotenen Elemente geändert. Außerdem ist die Darstellung der Liste von den Berechtigungen abhängig, über die Sie innerhalb der Registrierungsdomäne verfügen.

Detailgruppen

Auf der Registerkarte **Details** können Sie das Feld **Anzeigen** verwenden, um die gewünschte Attributgruppe auszuwählen. Über RA Desktop können jedoch nicht alle Details angezeigt werden. Manche Attribute sind in mehreren Gruppen enthalten. Sie können die folgenden Details anzeigen:

Basisattribute
Attribute, die einem Datenbanksatz standardmäßig zugeordnet sind.

Anforderungsattribute
Attribute, die zur Beschreibung des Registrierungsprozesses dienen.

Verarbeitungsattribute
Attribute, die zur Beschreibung der Verarbeitungsschritte dienen, die den Unternehmensregeln Ihres Unternehmens entsprechen. Diese Attribute umfassen auch das Attribut für die Widerrufbegründung.

Attribute für Schlüsselsicherungsanforderungen
Attribute, die mit Schlüsselsicherungsanforderungen in Zusammenhang stehen. Das Kennwort der gesicherten PKCS #12-Datei wird aufgeführt.

Aktionsprotokoll
Eine Tabelle mit allen Aktionen, die für eine Anforderung oder eine ausgeführte Anforderung durchgeführt wurden.

Status der Registrierungsanforderungen

Alle Statusangaben stellen Ereignisse im Aktionsprotokoll dar.

Folgende Anforderungsstatusarten stehen zur Verfügung:

Genehmigt
Die Registrierungsanforderung wurde genehmigt.

Abgeschlossen
Eine RA oder ein Registrator hat die Registrierungsanforderung entweder genehmigt oder nicht genehmigt. Für genehmigte Anforderungen wurde ein entsprechendes Zertifikat an den Benutzer übergeben.

Anmerkung: Dies ist der endgültige Anforderungsstatus für eine Registrierungsanforderung. Der Ausführungsstatus einer abgeschlossenen Anforderung verweist auf nachfolgende Aktionen und Ereignisse, die sich auf die Anforderung auswirken. Beispiel: Wird ein Zertifikat erneuert oder widerrufen, wird dies im Ausführungsstatus angegeben. Der Anforderungsstatus bleibt jedoch weiterhin ″Abgeschlossen″.

Anstehend
Die Registrierungsanforderung wurde möglicherweise bereits geprüft, die Genehmigung oder Zurückweisung steht jedoch weiterhin aus.

Empfangen
Die Registrierungsanforderung wurde empfangen.

Nicht genehmigt
Die Registrierungsanforderung wurde zurückgewiesen. Es wurde kein Zertifikat ausgestellt.

Folgende Ausführungsstatusarten stehen zur Verfügung:

Übergeben
Das Zertifikat wurde an die Web-Seite übergeben, auf der es vom Benutzer akzeptiert werden kann.

Übergabe bestätigt
Der Benutzer hat das Zertifikat auf den Web-Browser heruntergeladen.

Ausgestellt
Die Registrierungsanforderung wurde genehmigt und das Zertifikat wurde ausgestellt.

Nicht ausgestellt
Das Zertifikat wurde noch nicht ausgestellt. Dieser Status gibt nicht an, ob für die Anforderung eine Aktion durchgeführt wurde.

Erneuert
Das einem bestimmten Datensatz zugeordnete Zertifikat wurde erneuert. Hierdurch werden ein neuer Datensatz und ein neues Zertifikat generiert.

Widerrufen
Das einem bestimmten Datensatz zugeordnete Zertifikat wurde widerrufen und als ungültig definiert.

Hilfe für Registerkarten

Unter RA Desktop stehen die folgenden Hilfekomponenten auf allen Registerkarten zur Verfügung:

Statusbereich
In diesem Bereich unten auf der Registerkarte wird Folgendes angezeigt:

Hilfe für Feld
Wenn sich der Mauszeiger auf einem bestimmten Feld befindet, wird der zugehörige Hilfetext angezeigt.

Tivoli PKI-Nachrichten
Diese Nachrichten werden in einem Textfenster mit Blätterfunktion angezeigt und sind mit einem Symbol gekennzeichnet, das sie als Warnungen oder Fehlernachrichten ausweist.

Statusbalken
Dieser Balken zeigt den Fortschritt aller angeforderten Verarbeitungsoperationen an.

Hilfeknopf
Sie können auf diesen Knopf klicken, um Hilfetexte für die momentan verwendete Registerkarte anzuzeigen.

Anmerkung: Die angezeigte Hilfe enthält außerdem das Inhaltsverzeichnis für das Handbuch *RA Desktop*.Sie können alle Abschnitte in diesem Buch anzeigen. Klicken Sie hierzu auf den entsprechenden Eintrag im Inhaltsverzeichnis.

Zugehörige Abschnitte:

„Wechseln zwischen Registerkarten” auf Seite 19

JVM für Internet Explorer

Vor der Installation von RA Desktop für die Verwendung mit Internet Explorer müssen Sie das folgende Release von JVM (Java Virtual Machine) auf Ihrem System installieren:

- Release 5.00, ab Build 3167

Führen Sie einen der folgenden Arbeitsschritte aus, um festzustellen, welche Version von MS JVM auf Ihrem System installiert ist:

- Öffnen Sie die Java-Konsole über den Internet Explorer.
- Öffnen Sie eine DOS-Befehlszeile und geben Sie dort Folgendes ein: `jview`

Die angezeigte Versionsnummer sollte 5.00.3167 oder später sein.

Wenn Sie JVM erweitern müssen, können Sie das benötigte Release von der Microsoft Technologies für Java-Webseite herunterladen.

Tastaturalternativen zur Bedienung mit der Maus

Verwenden Sie die folgende Tabelle, wenn Sie RA Desktop ohne Maus bedienen möchten.

Cursor-/Eingabeposition		Taste/Tastenkombination
Allgemein		
	Erneute Initialisierung der Sitzung nach einer Zeitlimitüberschreitung.	Taste F5
	Verlassen von RA Desktop.	Strg-x
	Abrufen von Hilfe für die momentan angezeigte Registerkarte.	Taste F1
Arbeiten auf einer Registerkarte		
	Springen von den meisten Feldern auf die Registerkartenbezeichnung.	Strg-Aufwärtspfeiltaste
	Auswählen einer anderen Registerkarten-bezeichnung und Anzeigen dieser Registerkarte.	Rechtspfeiltaste zur Auswahl der nächsten Registerkarte. Linkspfeiltaste zur Auswahl der vorhergehenden Registerkarte.
	Blättern in einer Registerkarte.	Taste zur Abwärtsverschiebung des Bildes zum Abwärtsblättern, Taste zur Aufwärtsverschiebung des Bildes zum Aufwärtsblättern.
Arbeiten in Feldern		
	Springen von den meisten Feldern auf das nächste Feld.	Tabulatortaste
	Springen von den meisten Feldern auf das vor-hergehende Feld.	Umschalt- und Tabulatortaste
	Springen von einer Tabelle oder einem Text-bereich auf das nächste Feld.	Strg-Tabulatortaste
	Springen von einer Tabelle oder einem Text-bereich auf das vorhergehende Feld.	Strg-Umschalttaste-Tabulatortaste

Cursor-/Eingabeposition		Taste/Tastenkombination
Arbeiten in einer Tabelle		
	Sortieren von Zeilen nach Spaltenwerten.	Alt-*n*, wobei *n* für den Index der Spalte in der Anzeige steht. Beispiel: Um eine Tabelle nach der zweiten Spalte zu sortieren, drücken Sie die Tastenkombination Alt-2.
	Anpassen der Spaltengröße.	Ohne Maus nicht möglich.
	Springen von Zeile zu Zeile und dabei Zeilen auswählen.	Abwärtspfeiltaste zum Springen in die nächste Zeile, Aufwärtspfeiltaste zum Springen in die vorhergehende Zeile.
	Auswählen eines Zeilenbereichs.	Tastenkombination Umschalttaste-Aufwärtspfeiltaste oder Umschalttaste-Abwärtspfeiltaste zum Auswählen der Zeilen eines Bereichs.
	Auswählen nicht aufeinander folgender Zeilen.	Ohne Maus nicht möglich.
	Springen von Zelle zu Zelle innerhalb einer Zeile.	Mit der Tabulatortaste kann eine Zelle nach rechts gesprungen werden, mit der Tastenkombination Umschalttaste-Tabulatortaste eine Zelle nach links.
	Editieren der aktuellen Zelle, falls diese Operation zulässig ist.	Mit der Taste F2 kann eine Zelle zum Editieren geöffnet werden. Mit der Eingabetaste werden die Änderungen ans System übergeben und die Zelle wird verlassen. Mit der Abbruchtaste (Esc) kann die Zelle verlassen werden, ohne dass die Änderungen an das System übergeben werden.
Arbeiten mit den Elementen einer Liste		
	Öffnen einer Liste.	Aufwärts- oder Abwärtspfeiltaste.
	Springen durch eine Liste der Einträge.	Abwärtspfeiltaste zum Springen nach unten, Aufwärtspfeiltaste zum Springen nach oben.
	Auswählen eines Elements aus der Liste und Schließen der Liste.	Eingabetaste
	Schließen der Liste ohne Ändern der Auswahl.	Abbruchtaste (Esc)
	Verlassen und Springen zum nächsten Feld.	Tabulatortaste
Arbeiten mit einer Gruppe von Radioknöpfen (Gruppen werden als ein Feld interpretiert)		
	Springen von einem Radioknopf zum anderen und Auswählen des gewünschten Radioknopfes.	Abwärtspfeiltaste zum Springen nach unten, Aufwärtspfeiltaste zum Springen nach oben.
	Verlassen eines Feldes.	Tabulatortaste

Cursor-/Eingabeposition		Taste/Tastenkombination
Definieren eines Datums		
	Versetzen des Cursors im Datumsfeld.	Rechtspfeiltaste zum Versetzen des Cursors nach rechts, Linkspfeiltaste zum Versetzen des Cursors nach links.
	Öffnen des Kalenders über das Datumsfeld.	Aufwärts- oder Abwärtspfeiltaste
	Ändern der Jahresangabe im Kalender.	Strg-Taste zur Abwärtsverschiebung des Bildes zum Einstellen des nächsten Jahres, Strg-Taste zur Aufwärtsverschiebung des Bildes zum Einstellen des vorhergehenden Jahres.
	Ändern der Monatsangabe im Kalender.	Taste zur Abwärtsverschiebung des Bildes zum Einstellen des nächsten Monats, Taste zur Aufwärtsverschiebung des Bildes zum Einstellen des vorhergehenden Monats.
	Ändern der Datumsangabe im Kalender auf den Anfang oder das Ende eines Monats.	Taste für Pos1 zum Einstellen des Monatsanfangs, Endetaste zum Einstellen des Monatsendes.
	Ändern der Wochenangabe im Kalender.	Abwärtspfeiltaste zum Einstellen der nächsten, Aufwärtspfeiltaste zum Einstellen der vorhergehenden Woche.
	Ändern der Tagesangabe im Kalender.	Mit der Rechtspfeiltaste kann um einen Tag nach rechts, mit der Linkspfeiltaste um einen Tag nach links gesprungen werden.
	Springen auf das aktuelle Datum im Kalender.	Strg-Pos1
	Auswählen des hervorgehobenen Datums.	Eingabetaste
	Schließen des Kalenders ohne Auswahl eines Datums.	Abbruchtaste (Esc)
Arbeiten mit Befehlsknöpfen		
	Springen auf einen Befehlsknopf.	Tabulatortaste
	Ausführen des gewünschten Befehls.	Leertaste oder Eingabetaste.

Fehlerbehebung

Dieser Abschnitt enthält Richtlinien zur Verwendung sowie Empfehlungen zur Fehlerbehebung für die Ausführung von RA Desktop.

- Wenn Sie Microsoft Internet Explorer verwenden, treten möglicherweise folgende Fehler im Zusammenhang mit der Benutzerschnittstelle auf:
  - Wenn Sie eine Fehlernachricht erhalten, die sich auf SSL bezieht, wählen Sie **Extras → Internetoptionen** aus. Wählen Sie im Fenster 'Internetoptionen' die Registerkarte **Erweitert** aus und klicken Sie auf den Knopf **Standard wiederherstellen**. Dadurch wird SSL 3.0 erneut aktiviert. Klicken Sie auf **OK** und schließen Sie alle noch geöffneten Internet Explorer-Fenster. Starten Sie RA Desktop erneut.
  - Die Ergebnistabelle enthält keine Einträge, obwohl eine Abfrage eine bestimmte Anzahl von Einträgen zurückgegeben hat.

    Dieser Fehler ist auf eine Verzögerung beim Ausfüllen des Applets zurückzuführen. Sie können den Fehler beheben, indem Sie auf den Knopf **Aktualisieren** des verwendeten Browsers klicken, um das Applet erneut zu starten.
  - Die Elemente im kombinierten Fenster können nicht mit der Maus ausgewählt werden.

    Dieser Fehler tritt auf, wenn sich ein Dialogfenster außerhalb des Applet-Bereichs befindet. Er betrifft die Listen- und Detailteilanzeige, wenn Sie eines der kombinierten Fenster auswählen, ohne im Fenster vorwärts zu blättern. Dadurch wird das kombinierte Fenster unterhalb der unteren Begrenzung des Applets angezeigt.

    Sie können diesen Fehler umgehen, indem Sie das kombinierte Fenster über die Tastatur auswählen. Verwenden Sie den Aufwärts- bzw. Abwärtspfeil und drücken Sie anschließend die Eingabetaste oder die Leertaste. Alternativ dazu können Sie auch im Fenster blättern, um das kombinierte Fenster höher und weiter zur Applet-Mitte hin zu positionieren.

Glossar

In diesem Glossar werden alle Termini und Abkürzungen definiert, die in diesem Handbuch verwendet werden und die möglicherweise neu oder unbekannt und von Bedeutung sind.

Numerische Einträge

4758 PCI Cryptographic Coprocessor
Eine programmierbare, manipulationssensitive PCI-Bus-Verschlüsselungskarte, die die Ausführung von DES- und RSA-Verschlüsselungsoperationen mit hoher Geschwindigkeit ermöglicht. Die Verschlüsselungsprozesse werden in einem gesicherten und abgegrenzten Bereich auf der Karte ausgeführt. Die Karte entspricht den strengen Anforderungen des FIPS PUB 140-1 Level 4-Standards. In dem gesicherten und abgegrenzten Bereich kann Software ausgeführt werden. Der SET-Standard kann beispielsweise zur Verarbeitung von Kreditkartentransaktionen genutzt werden.

A

Abstract Syntax Notation One (ASN.1)
Eine ITU-Notation, die zum Definieren der Syntax von Informationsdaten benutzt wird. Sie definiert eine Reihe einfacher Datentypen und gibt eine Notation für die Identifizierung dieser Typen und die Angabe von Werten für diese Typen an. Diese Notationen können verwendet werden, wenn es erforderlich ist, die abstrakte Syntax von Informationen zu definieren, ohne damit die Art der Verschlüsselung dieser Informationen für die Übertragung zu beeinträchtigen.

ACL
Access Control List - Zugriffssteuerungsliste.

Aktionsprotokoll
Die Aufzeichnung aller Ereignisse, die während der gesamten Gültigkeitsdauer eines Identitätsnachweises aufgetreten sind.

American National Standard Code for Information Interchange (ASCII)
Der Standardcode, der für den Austausch von Informationen zwischen Datenverarbeitungssystemen, DFV-Systemen und zugehöriger Hardware verwendet wird. ASCII verwendet einen codierten Zeichensatz, der aus Zeichen von 7 Bit Länge (bzw. 8 Bit bei Paritätsprüfung) besteht. Der Zeichensatz besteht hierbei aus Steuerzeichen und Schriftzeichen.

American National Standards Institute (ANSI)
Eine Organisation, die die Verfahrensweisen definiert, mit deren Hilfe akkreditierte Organisationen freiwillig eingehaltene Industriestandards in den Vereinigten Staaten festlegen und verwalten. Ihr gehören Hersteller, Verbraucher und allgemeine Interessenvertretungen an.

Anforderungs-ID
Ein aus 24 bis 32 Zeichen bestehender ASCII-Wert, der zur eindeutigen Identifikation einer Zertifikatsanforderung gegenüber der RA dient. Dieser Wert kann bei der Transaktion für die Zertifikatsanforderung verwendet werden, um den Status der Anforderung oder des zugehörigen Zertifikats abzurufen.

ANSI
American National Standards Institute.

Applet
Ein in der Programmiersprache Java geschriebenes Computerprogramm, das innerhalb eines Java-kompatiblen Webbrowsers ausgeführt werden kann. Wird auch als Java-Applet bezeichnet.

Art
Siehe Objektart.

ASCII
American National Standard Code for Information Interchange.

ASN.1
Abstract Syntax Notation One.

Asymmetrische Verschlüsselung
Ein Verschlüsselungsverfahren, das zur Ver- und Entschlüsselung unterschiedliche, asymmetrische Schlüssel verwendet. Jedem Benutzer wird hierbei ein Schlüsselpaar zugeordnet, das einen allgemeinen, für alle zugänglichen Schlüssel und einen privaten Schlüssel umfasst, der nur dem jeweiligen Benutzer bekannt ist. Eine gesicherte Transaktion kann ausgeführt werden, wenn der öffentliche Schlüssel sowie der zugehörige private Schlüssel übereinstimmen. In diesem Fall kann die Transaktion entschlüsselt werden. Dieses Verfahren wird auch als Verschlüsselung auf der Basis von Schlüsselpaaren bezeichnet. *Gegensatz zu* Symmetrische Verschlüsselung.

Asynchrone Übertragung
Ein Übertragungsmodus, bei dem Sender und Empfänger nicht gleichzeitig vorhanden sein müssen.

Authentifizierung
Der Vorgang, bei dem die Identität eines Teilnehmers an einer Übertragung zuverlässig überprüft wird.

B

Base64-Verschlüsselung
Ein häufig verwendetes Verfahren bei der Übertragung von Binärdaten mit MIME.

Basic Encoding Rules (BER)
Die Regeln, die in ISO 8825 für die Verschlüsselung von in ASN.1 beschriebenen Dateneinheiten angegeben sind. Die Regeln geben das Verschlüsselungsverfahren, jedoch nicht die abstrakte Syntax an.

Benutzerauthentifizierung
Der Prozess, mit dem überprüft wird, ob der Absender einer Nachricht die berechtigte Person ist, als die er sich ausgibt. Der Prozess überprüft außerdem, ob ein Kommunikationsteilnehmer auch tatsächlich mit dem erwarteten Endbenutzer oder System in Verbindung steht.

BER
Basic Encoding Rules.

Berechtigung
Die Erlaubnis, auf eine Ressource zuzugreifen.

Bestreiten
Etwas als unwahr zurückweisen. Dies ist z. B. dann der Fall, wenn ein Benutzer abstreitet, eine bestimmte Nachricht gesendet oder eine bestimmte Anforderung übergeben zu haben.

Browser
Siehe Web-Browser.

Browser-Zertifikat
Ein digitales Zertifikat, das auch als Zertifikat der Client-Seite bezeichnet wird. Es wird von einem CA über einen für SSL aktivierten Web-Server ausgestellt. Die Schlüssel in einer verschlüsselten Datei ermöglichen dem Eigner des Zertifikats das Verschlüsseln, Entschlüsseln und Unterzeichnen von Daten. Normalerweise werden diese Schlüssel im Web-Browser gespeichert. In bestimmten Anwendungen können die Schlüssel auf Smart-Cards oder anderen Speichermedien gespeichert werden. *Siehe auch* Digitales Zertifikat.

Bytecode
Maschinenunabhängiger Code, der mit dem Java-Compiler generiert und mit dem Java-Interpreter ausgeführt wird.

C

CA
Certificate Authority - Zertifikatsaussteller.

CA-Hierarchie
Bei Tivoli PKI eine Sicherungsstruktur, bei der ein CA auf der höchsten Ebene positioniert ist. Anschließend können bis zu vier weitere Ebenen mit untergeordneten CAs definiert werden. Wenn Benutzer oder Server bei einem

Zertifikatsaussteller registriert werden, wird ihnen ein von diesem Aussteller unterzeichnetes Zertifikat zugeordnet. Außerdem übernehmen sie die Zertifizierungshierarchie der übergeordneten Ebenen.

CA-Server
Der Server für die CA-Komponente von Tivoli PKI.

CAST-64
Ein Block-Cipher-Algorithmus, der mit einer Blockgröße von 64 Bit und einem 6-Bit-Schlüssel arbeitet. Er wurde von Carlisle Adams und Stafford Tavares entwickelt.

CA-Zertifikat
Ein Zertifikat, das vom Web-Browser eines Benutzers auf dessen Anforderung hin von einem nicht identifizierten CA akzeptiert wird. Der Browser kann dann dieses Zertifikat verwenden, um für die Kommunikation mit Servern, die über Zertifikate dieses CAs verfügen, eine Authentifizierung durchzuführen.

CCA
Common Cryptographic Architecture von IBM.

CDSA
Common Data Security Architecture.

CGI
Common Gateway Interface.

Client
(1) Eine Funktionseinheit, die gemeinsam benutzte Services von einem Server empfängt. (2) Ein Computer oder Programm, der/das Services von einem anderen Computer oder Programm anfordert.

Client/Server
Ein Modell für die verteilte Verarbeitung, bei dem ein Programm an einem Standort eine Anforderung an ein Programm an einem anderen Standort sendet und auf eine Antwort wartet. Das anfordernde Programm wird als Client, das antwortende als Server bezeichnet.

Codeunterzeichnung
Ein Verfahren zum Unterzeichnen ausführbarer Programme mit einer digitalen Unterschrift. Die Codeunterzeichnung dient zur Verbesserung der Zuverlässigkeit von Softwarekomponenten, die über das Internet verteilt werden.

Common Cryptographic Architecture (CCA)
IBM Software, die einen konsistenten Verschlüsselungsansatz auf den wichtigsten IBM Computerplattformen bietet. Sie unterstützt Anwendungssoftware, die in einer Vielzahl von Programmiersprachen geschrieben wurde. Die Anwendungssoftware kann hierbei die CCA-Services aufrufen, um eine breite Palette kryptografischer Funktionen (einschließlich der DES- und der RSA-Verschlüsselung) auszuführen.

Common Data Security Architecture (CDSA)
Eine Initiative zum Definieren eines umfassenden Ansatzes für Sicherheitsservices und Sicherheitsverwaltungsoperationen bei computerbasierten Sicherheitsanwendungen. Diese Architektur wurde von Intel entworfen und dient dazu, Computerplattformen für Anwendungen sicherer zu gestalten.

Common Gateway Interface (CGI)
Ein Standardverfahren zum Übertragen von Informationen zwischen Web-Seiten und Web-Servern.

CRL
Certificate Revocation List - Zertifikatswiderrufsliste.

CRL-Veröffentlichungsintervall
Dieses Intervall wird in der CA-Konfigurationsdatei definiert und gibt das Zeitintervall zwischen zwei Veröffentlichungen der Zertifikatswiderrufsliste im Directory an.

D

Dämon

Ein Programm, das Tasks im Hintergrund ausführt. Es wird implizit aufgerufen, wenn eine Bedingung auftritt, die die Hilfe des Dämons erforderlich macht. Es ist nicht erforderlich, dass der Benutzer über die Ausführung des Dämons unterrichtet wird, da der Dämon normalerweise vom System automatisch gestartet wird. Ein Dämon kann über eine unbegrenzte Zeit hinweg ausgeführt oder vom System in bestimmten Zeitintervallen erneut generiert werden.

Der Terminus (englisch *demon*) stammt aus der Mythologie. Später wurde er aber als Akronym für den Ausdruck ″Disk And Execution MONitor″ (Platten- und Ausführungsüberwachungsprogramm) erklärt.

Data Encryption Standard (DES)

Eine Verschlüsselungs-Block-Cipher, die 1977 von der US-Regierung als offizieller Standard definiert und übernommen wurde. Dieser Standard wurde ursprünglich von IBM entwickelt. DES wurde seit seiner Veröffentlichung umfassend untersucht und stellt ein allgemein bekanntes und häufig verwendetes Verschlüsselungssystem zur Verfügung.

Bei DES handelt es sich um ein symmetrisches Verschlüsselungssystem. Um es für die Datenübertragung einzusetzen, müssen sowohl der Sender als auch der Empfänger den selben, geheimen Schlüssel kennen. Dieser Schlüssel wird zum Ver- und Entschlüsseln der Nachricht verwendet. DES kann außerdem zur Durchführung von Verschlüsselungsoperationen für einzelne Benutzer eingesetzt werden, z. B. zum Speichern von verschlüsselten Dateien auf einer Festplatte. DES arbeitet mit einer Blockgröße von 64 Bit und verwendet für die Verschlüsselung einen 56-Bit-Schlüssel. Ursprünglich wurde dieser Standard für die Hardwareimplementierung entwickelt. DES wird von NIST alle fünf Jahre erneut als offizieller Verschlüsselungsstandard der US-Regierung zertifiziert.

Datenspeicherbibliothek (DL)

Ein Modul, das den Zugriff auf permanente Datenspeicher mit Zertifikaten, CRLs, Schlüsseln, Regeln und anderen sicherheitsrelevanten Objekten ermöglicht.

DEK

Document Encryption Key = Dokumentverschlüsselungsschlüssel.

DER

Distinguished Encoding Rules.

DES

Data Encryption Standard.

Diffie-Hellman

Ein Verfahren zur Datenverschlüsselung, das auf der Verwendung eines gemeinsamen Schlüssels auf einem nicht gesicherten Medium basiert und nach seinen Erfindern (Whitfield Diffie und Martin Hellman) benannt wurde.

Digitales Zertifikat

Ein elektronischer Identitätsnachweis, der von einer zuverlässigen Stelle für eine Person oder Entität ausgestellt wird. Jedes Zertifikat ist mit dem privaten Schlüssel des CAs unterzeichnet. Es bürgt für die Identität einer Person, eines Unternehmens oder einer Organisation.

Abhängig vom Aufgabenbereich des CAs kann das Zertifikat die Berechtigung seines Eigners bestätigen, e-Business-Transaktionen über das Internet auszuführen. In gewisser Weise hat ein digitales Zertifikat eine ähnliche Funktion wie ein Führerschein oder ein Meisterbrief. Es bestätigt, dass der Inhaber des entsprechenden privaten Schlüssels berechtigt ist, bestimmte e-Business-Aktivitäten auszuführen.

Ein Zertifikat enthält Informationen über die Entität, die von ihm zertifiziert wird, gibt an, ob es sich um eine Person, eine Maschine oder ein Computerprogramm handelt und enthält als Teil dieser Informationen den zertifizierten öffentlichen Schlüssel dieser Entität.

Digitale Unterschrift

Eine codierte Nachricht, die an Dokumente oder Daten angefügt wird, und die Identität des Absenders nachweist. Eine digitale Unterschrift gewährleistet ein höheres Maß an Sicherheit als eine physische Unterschrift, da es sich hierbei nicht lediglich um einen verschlüsselten Namen oder eine Reihe einfacher Identifikationscodes handelt. Eine digitale Unterschrift enthält eine verschlüsselte Zusammenfassung der unterzeichneten Nachricht. Durch das Anfügen einer digitalen Unterschrift an eine Nachricht lässt sich der Absender also zweifelsfrei feststellen. (Die Unterschrift kann nur mit Hilfe des Schlüssels des Absenders erstellt werden.) Außerdem ermöglicht sie die Absicherung des Inhalts der unterzeichneten Nachricht, da die verschlüsselte Nachrichtenzusammenfassung mit dem Nachrichteninhalt übereinstimmen muss. Andernfalls wird die Unterschrift nicht als gültig identifiziert. Eine digi-

tale Unterschrift kann also nicht von einer Nachricht kopiert und für eine andere Nachricht verwendet werden, da sonst die Zusammenfassung (Hash-Code) nicht übereinstimmen würde. Alle Änderungen an der unterzeichneten Nachricht führen automatisch zum Verlust der Gültigkeit der Unterschrift.

Digitale Zertifizierung
Siehe Zertifizierung.

Digital Signature Algorithm (DSA)
Ein auf öffentlichen Schlüsseln basierender Algorithmus, der zum Standard für digitale Unterschriften (Digital Signature Standard = DSS) gehört. Er kann nur für digitale Unterschriften, jedoch nicht für die Verschlüsselung verwendet werden.

Directory
Eine hierarchische Struktur, die als globales Repository für Informationen zur Datenkommunikation (wie beispielsweise E-Mail oder Austausch von verschlüsselten Daten) konzipiert ist. Im Directory werden bestimmte Elemente gespeichert, die für die PKI-Struktur (PKI = Public Key Infrastructure) unbedingt erforderlich sind. Hierzu gehören die folgenden Elemente: öffentliche Schlüssel, Zertifikate und Zertifikatswiderrufslisten (CRLs).
Die Daten im Directory sind hierarchisch in einer Baumstruktur organisiert, wobei die oberste Ebene der Baumstruktur das Root-Verzeichnis ist. Häufig stehen Organisationen einer höheren Ebene für einzelne Länder, Regierungen oder Unternehmen. Benutzer oder Einheiten werden im Allgemeinen als ″Blätter″ einer solchen Baumstruktur dargestellt. Diese Benutzer, Organisationen, Standorte, Länder und Einheiten haben jeweils ihren eigenen Eintrag. Jeder Eintrag besteht aus Attributen, denen verschiedene Typen zugewiesen sind. Diese enthalten Informationen zu den Objekten, für die der jeweilige Eintrag steht.
Jeder Eintrag im Directory ist mit einem zugeordneten registrierten Namen (DN = Distinguished Name) verbunden. Dieser ist eindeutig, wenn der Eintrag ein Attribut umfasst, das für das tatsächliche Objekt als eindeutig bekannt ist. Im folgenden DN-Beispiel wurde als Land (C = Country) US, als Unternehmen (O = Organization) IBM, als Unternehmenseinheit (OU = Organizational Unit) Trust und als allgemeiner Name (CN = Common Name) der Wert CA1 angegeben.

```
C=US/O=IBM/OU=Trust/CN=CA1
```

Directory-Server
In Tivoli PKI das IBM SecureWay Directory. Dieses Directory unterstützt die LDAP-Standards und verwendet DB2 als Basissystem.

Distinguished Encoding Rules (DER)
Durch DER werden bestimmte Einschränkungen für BER definiert. Mit DER kann genau ein bestimmter Verschlüsselungstyp aus den verfügbaren und auf der Basis der Verschlüsselungsregeln als zulässig definierten Typen ausgewählt werden. Hierdurch werden alle Senderoptionen eliminiert.

DL
Data Storage Library = Datenspeicherbibliothek.

DN
Distinguished Name - Registrierter Name.

Dokumentverschlüsselungsschlüssel (DEK)
Normalerweise ein symmetrischer Ver-/Entschlüsselungsschlüssel, z. B. DES.

Domäne
Siehe Sicherheitsdomäne *und* Registrierungsdomäne.

DSA
Digital Signature Algorithm.

E

e-Business
Das Durchführen geschäftlicher Transaktionen über Netze und Computer, z. B. der Kauf und Verkauf von Waren und Dienstleistungen sowie der Transfer von Zahlungsmitteln mit Hilfe der digitalen Kommunikation.

e-Commerce
Unternehmensübergreifende Transaktionen wie beispielsweise der Kauf und Verkauf von Waren und Dienstleistungen (zwischen Unternehmen und ihren Kunden, Lieferanten, Subunternehmen und anderen) über das Internet. E-Commerce stellt einen Kernbestandteil des e-Business dar.

Endentität
Der Gegenstand eines Zertifikats, bei dem es sich nicht um einen CA handelt.

Entschlüsseln
Den Verschlüsselungsprozess rückgängig machen.

Exemplar
Bei DB2 bezeichnet man als Exemplar eine logische Datenbankverwaltungsumgebung zum Speichern von Daten und zum Ausführen von Anwendungen. Es ermöglicht die Definition einer allgemeinen Gruppe von Konfigurationsparametern für verschiedene Datenbanken.

Extranet
Ein Netz, das auf dem Internet basiert und eine ähnliche Technologie einsetzt. Unternehmen beginnen momentan mit dem Einsatz des Web Publishings, elektronischen Handels und der Nachrichtenübertragung sowie der Verwendung von Groupware für verschiedene Gruppen von Kunden, Partnern und internen Mitarbeitern.

F

File Transfer Protocol (FTP)
Ein Client/Server-Protokoll im Internet, das zum Übertragen von Dateien zwischen Computern benutzt wird.

Firewall
Ein Gateway zwischen Netzen, der den Informationsfluss zwischen diesen einschränkt. Normalerweise dienen Firewalls dem Schutz interner Netze gegen die nicht berechtigte Verwendung durch externe Personen.

FTP
File Transfer Protocol.

G

Gateway
Eine Funktionseinheit, mit deren Hilfe nicht kompatible Netze oder Anwendungen Daten austauschen können.

Gegenseitige Zertifizierung
Ein Trust-Modell, bei dem ein CA für einen anderen CA ein Zertifikat ausstellt, das den öffentlichen Schlüssel enthält, der dem entsprechenden privaten Unterschriftsschlüssel zugeordnet ist. Ein gegenseitig zertifiziertes Zertifikat ermöglicht Client-Systemen oder Endentitäten in einer Verwaltungsdomäne die sichere Kommunikation mit Client-Systemen oder Endentitäten in einer anderen Domäne.

Gesicherte Computerbasis (TCB)
Die Software- und Hardwareelemente, die zur Umsetzung der Computersicherheitsregeln eines Unternehmens verwendet werden. Alle Elemente oder Teilelemente, die zur Implementierung der Sicherheitsregeln eingesetzt werden können, sind sicherheitsrelevant und Bestandteil der TCB. Bei der TCB handelt es sich um ein Objekt, das durch die Sicherheitsperipherie begrenzt wird. Die Mechanismen, die zur praktischen Umsetzung der Sicherheitsregeln eingesetzt werden, dürfen nicht umgangen werden können und müssen verhindern, dass Programme Zugriff auf Systemprivilegien erlangen können, für die sie nicht berechtigt sind.

H

Hierarchie
Die Organisation der Zertifizierungsstellen (CA) in einer Trust-Kette. Die Kette beginnt mit dem selbst unterzeichnenden CA bzw. der Root der Roots am Anfang und endet mit dem CA, der Zertifikate für Endbenutzer ausstellt.

Höchster CA
Der CA, der innerhalb der PKI-CA-Hierarchie die höchste Position einnimmt.

HTML
Hypertext Markup Language.

HTTP
Hypertext Transaction Protocol.

HTTP-Server
Ein Server, der die Web-gestützte Kommunikation mit Browsern und anderen Programmen im Netz steuert.

Hypertext
Textsegmente, die einzelne oder mehrere Wörter umfassen oder Bilder enthalten, auf die der Leser mit der Maus klicken kann, um ein anderes Dokument aufzurufen und anzuzeigen. Diese Textsegmente werden als Hyperlinks bezeichnet. Ruft der Leser diese anderen Dokumente auf, stellt er zu diesen eine Hyperlink-Verbindung her.

Hypertext Markup Language (HTML)
Eine Formatierungssprache für das Codieren von Web-Seiten. HTML basiert auf SGML (Standard Generalized Markup Language).

Hypertext Transaction Protocol (HTTP)
Ein Client/Server-Protokoll für das Internet, mit dem Hypertext-Dateien im Web übertragen werden.

I

ICL
Issued Certificate List - Liste der ausgestellten Zertifikate.

Identitätsnachweis
Vertrauliche Informationen, die verwendet werden, um beim Austausch von Daten während der Authentifizierung die eigene Identität zu belegen. In Network Computing-Umgebungen ist die am häufigsten verwendete Form des Identitätsnachweises ein Zertifikat, das von einem CA erstellt und unterzeichnet wurde.

IniEditor
Bei Tivoli PKI ein Tool, mit dem Konfigurationsdateien editiert werden können.

Integrität
Ein System schützt seine Datenintegrität, wenn es die Änderung dieser Daten durch nicht berechtigte Personen verhindert. (Im Gegensatz hierzu versteht man unter dem Schutz der Vertraulichkeit von Daten, wenn verhindert wird, dass diese unberechtigten Personen zugänglich gemacht werden.)

Integritätsprüfung
Die Prüfung der Protokolleinträge, die für Transaktionen mit externen Komponenten aufgezeichnet wurden.

International Standards Organization (ISO)
Eine internationale Organisation, die Standards für eine breite Palette von Industriebereichen, z. B. auch für Computernetzprotokolle, entwickelt und veröffentlicht.

International Telecommunication Union (ITU)
Eine internationale Organisation, in der Verwaltungs- und private Industriebereiche globale Datenfernübertragungsnetze und -services koordinieren. Bei der Veröffentlichung von Informationen zur Datenfernübertragungstechnologie sowie den entsprechenden Regelwerken und Standards nimmt sie eine führende Position ein.

Interne Struktur
Siehe Schema.

Internet
Ein weltweiter Verbund von Netzen, die die elektronische Verbindung zwischen Computern und die Kommunikation zwischen den Computern über Softwareeinrichtungen wie elektronische Post (E-Mail) oder Web-Browser ermöglichen. So sind beispielsweise die meisten Universitäten in ein Netz eingebunden, das seinerseits eine Verbindung zu anderen ähnlichen Netzen hat, die zusammen das Internet bilden.

Internet Engineering Task Force (IETF)
Eine Gruppe, die sich schwerpunktmäßig mit dem Entwickeln und Definieren von Protokollen für das Internet befasst. Sie repräsentiert eine internationale Gruppe von Netzdesignern, -bedienern, -herstellern und -forschern. Die Aufgabe der IETF ist die Entwicklung der Internet-Architektur sowie die Gewährleistung der reibungslosen Verwendung des Internets.

Intranet
Ein Netz innerhalb eines Unternehmens, das sich im Allgemeinen hinter Firewalls befindet. Es basiert auf dem Internet und setzt eine ähnliche Technologie ein. Vom technischen Standpunkt aus ist ein Intranet eine Erweiterung des Internets. Zu den in beiden Netzen benutzten Komponenten gehören z. B. HTML und HTTP.

IPSec
Ein von der IETF entwickelter IPS-Standard (IPS = Internet Protocol Security). IPSec ist ein Protokoll der Vermittlungsschicht, das entwickelt wurde, um Services für die Gewährleistung der Sicherheit bei der Verschlüsselung zur Verfügung zu stellen, die kombinierte Funktionen zur Authentifizierung, Sicherung der Integrität, Zugriffssteuerung und Wahrung der Vertraulichkeit flexibel unterstützen. Aufgrund seiner leistungsfähigen Funktionen bei der Authentifizierung wurde dieser Standard von vielen Lieferanten von VPN-Produkten als Protokoll zum Aufbau sicherer Punkt-zu-Punkt-Verbindungen im Internet übernommen.

ISO
International Standards Organization.

ITU
International Telecommunication Union.

J

Java
Von Sun Microsystems, Incorporated, entwickelte plattformunabhängige Computertechnologien, die für den Netzbetrieb optimiert sind. Die Java-Umgebung besteht aus dem Java-Betriebssystem (Java-OS), den virtuellen Maschinen für verschiedene Plattformen, der objektorientierten Java-Programmiersprache und einer Reihe von Klassenbibliotheken.

Java-Anwendung
Ein eigenständiges Programm, das in der Java-Sprache geschrieben wurde. Es wird außerhalb eines Web-Browsers ausgeführt.

Java-Applet
Siehe Applet. *Gegensatz zu* Java-Anwendung.

Java-Klasse
Eine Einheit des Java-Programmcodes.

Java-Sprache
Eine von Sun Microsystems entwickelte Programmiersprache, die speziell für die Verwendung in Applet- und Agent-Anwendungen konzipiert wurde.

Java Virtual Machine (JVM)
Der Teil der Java-Laufzeitumgebung, der zum Interpretieren von Bytecodes eingesetzt wird.

K

KeyStore (Schlüsselspeicher)
Eine DL zum Speichern von Identitätsnachweisen für Tivoli PKI-Komponenten, z. B. Schlüssel und Zertifikate, in einem verschlüsselten Format.

Klartext
Nicht verschlüsselte Daten. *Synonym zu* unverschlüsselter Text.

Klasse

Beim objektorientierten Entwurf bzw. bei der objektorientierten Programmierung eine Gruppe von Objekten, die über eine gemeinsame Definition verfügen und aus diesem Grund mit denselben Merkmalen, Verarbeitungsoperationen und Funktionsweisen arbeiten.

Kryptographie

Bei der Sicherung von Computern die Prinzipien, Verfahren und Methoden zur Verschlüsselung von unverschlüsseltem und zur Entschlüsselung von verschlüsseltem Text.

L

LDAP

Lightweight Directory Access Protocol.

Lightweight Directory Access Protocol (LDAP)

Ein Protokoll, mit dem auf das Directory zugegriffen werden kann.

Liste der ausgestellten Zertifikate (ICL)

Eine vollständige Liste der ausgestellten Zertifikate sowie deren aktueller Status. Die Zertifikate sind anhand der Seriennummer und des Status indexiert. Diese Liste wird vom CA verwaltet und in der CA-Datenbank gespeichert.

M

MAC

Message Authentication Code - Nachrichtenauthentifizierungscode.

MD4

Eine Nachrichtenauszugs-Hash-Funktion auf 128-Bit-Basis, die von Ron Rivest entwickelt wurde. Ihre Geschwindigkeit übersteigt die von MD2 um ein Mehrfaches.

MD5

Eine unidirektionale Nachrichtenauszugs-Hash-Funktion, die von Ron Rivest entwickelt wurde. Sie stellt eine verbesserte Version von MD4 dar. MD5 verarbeitet Eingabetext in 512-Bit-Blöcken, die in 16 32-Bit-Unterblöcke aufgeteilt werden. Die Ausgabe des Algorithmus ist eine Gruppe von vier 32-Bit-Blöcken, die verkettet werden und so einen 128-Bit-Hash-Wert bilden. Diese Funktion wird ebenfalls zusammen mit MD2 in dem PEM-Protokollen verwendet.

MD2

Eine Nachrichtenauszugs-Hash-Funktion auf 128-Bit-Basis, die von Ron Rivest entwickelt wurde. Sie wird zusammen mit MD5 in den PEM-Protokollen verwendet.

Modulus

In dem auf öffentlichen Schlüsseln basierenden RSA-Verschlüsselungssystem das Produkt (n) aus zwei hohen Primzahlen: p und q. Die optimale Größe für einen RSA-Modulus hängt von den individuellen Sicherheitsanforderungen ab. Je größer der Modulus, desto höher die Sicherheit. Die momentan von den RSA Laboratories empfohlenen Schlüsselgrößen hängen vom geplanten Einsatz des Schlüssels ab. Hierbei werden 768 Bit für Schlüssel zum persönlichen Gebrauch, 1024 Bit für den Unternehmensbereich und 2048 Bit für extrem wertvolle Schlüssel wie z. B. CA-Schlüsselpaare angegeben. Ein 768-Bit-Schlüssel wird voraussichtlich bis mindestens zum Jahr 2004 sicher sein.

Multipurpose Internet Mail Extensions (MIME)

Eine frei verfügbare Gruppe von Spezifikationen, die den Austausch von Text in Sprachen mit unterschiedlichen Zeichensätzen ermöglicht. Diese Spezifikationen unterstützen auch den Austausch von Multimedia-E-Mail zwischen unterschiedlichen Computersystemen, die Internet-Mail-Standards verwenden. So können E-Mail-Nachrichten beispielsweise andere Zeichensätze als den US-ASCII-Satz sowie erweiterten Text, Bilder oder Tondaten enthalten.

N

Nachrichtenauszug
Eine irreversible Funktion, bei der auf der Basis einer Nachricht beliebiger Länge eine Datenmenge mit fester Länge generiert wird. Bei MD5 handelt es sich z. B. um einen Nachrichtenauszugsalgorithmus.

Nachrichtenauthentifizierungscode (MAC)
Ein geheimer Schlüssel, der von Sender und Empfänger gemeinsam benutzt wird. Der Sender authentifiziert sich und der Empfänger prüft die hierbei zur Verfügung gestellten Daten. Bei Tivoli PKI werden MAC-Schlüssel für CA- und Prüfkomponenten in den KeyStores gespeichert.

National Security Agency (NSA)
Die offizielle Sicherheitsbehörde der US-Regierung.

NIST
National Institute of Standards and Technology, früher NBS (National Bureau of Standards). Aufgabe dieses Instituts ist die Unterstützung offener Standards und der Interoperabilität in den verschiedenen Bereichen der Computerbranche.

NLS
National Language Support - Unterstützung in der Landessprache.

NSA
National Security Agency.

O

Objekt
Beim objektorientierten Design oder bei der objektorientierten Programmierung eine abstrakte Entität, die zur Abgrenzung bestimmter Daten und der zugehörigen Operationen dient. *Siehe auch* Klasse.

Objektart
Die Art von Objekt, die im Directory gespeichert werden kann. Beispiele sind eine Firma, ein Konferenzraum, eine Einheit, eine Person, ein Programm oder ein Prozess.

Objekt-ID (OID)
Ein von einer Verwaltungsfunktion zugeordneter Datenwert, der den in ASN.1 definierten Typ aufweist.

ODBC
Open Database Connectivity.

Öffentlicher Schlüssel
In einem Paar aus einem öffentlichen und einem privaten Schlüssel steht dieser Schlüssel anderen Benutzern zur Verfügung. Er ermöglicht diesen Benutzern die Weiterleitung einer Transaktion an den Eigner des Schlüssels sowie die Prüfung einer digitalen Unterschrift. Mit einem öffentlichen Schlüssel verschlüsselte Daten können nur mit dem entsprechenden privaten Schlüssel entschlüsselt werden. *Gegensatz zu* Privater Schlüssel. *Siehe auch* Schlüsselpaar aus öffentlichem und privatem Schlüssel.

Open Database Connectivity (ODBC)
Ein Standard für den Zugriff auf unterschiedliche Datenbanksysteme.

Open Systems Interconnect (OSI)
Der Name der von ISO genehmigten Computernetzstandards.

OSI
Open Systems Interconnect.

P

PC-Karte
Eine mit einer Smart-Card vergleichbare Einheit, die auch als PCMCIA-Karte bezeichnet wird. Sie ist etwas größer als eine Smart-Card und verfügt im Allgemeinen über eine höhere Kapazität.

PEM
Privacy-Enhanced Mail.

PKCS
Public Key Cryptography Standards.

PKCS #1
Siehe Public Key Cryptography Standards.

PKCS #7
Siehe Public Key Cryptography Standards.

PKCS #10
Siehe Public Key Cryptography Standards.

PKCS #11
Siehe Public Key Cryptography Standards.

PKCS #12
Siehe Public Key Cryptography Standards.

PKI
Public Key Infrastructure.

PKIX
PKI auf X.509v3-Basis.

PKIX Certificate Management Protocol (PKIX CMP)
Ein Protokoll, das Verbindungen mit PKIX-kompatiblen Anwendungen ermöglicht. PKIX CMP verwendet als primäres Transportverfahren TCP/IP, es ist jedoch eine Abstraktionsebene oberhalb der Sockets-Schicht vorhanden. Hierdurch können zusätzliche Datenübertragungsoperationen mit Sendeaufrufen (Polling) unterstützt werden.

PKIX CMP
PKIX Certificate Management Protocol.

PKIX-Empfangseinheit
Der öffentliche HTTP-Server, der von einer bestimmten Registrierungsdomäne verwendet wird, um Anforderungen der Client-Anwendung von Tivoli PKI zu empfangen.

Privacy-Enhanced Mail (PEM)
Der vom Internet Architect Board (IAB) genehmigte Internet-Standard für die verbesserte Wahrung der Vertraulichkeit, der die sichere Übertragung elektronischer Post (E-Mail) über das Internet ermöglicht. Die PEM-Protokolle regeln Verschlüsselung, Authentifizierung, Nachrichtenintegrität und Schlüsselverwaltung.

Privater Schlüssel
In einem Paar aus einem öffentlichen und einem privaten Schlüssel steht dieser Schlüssel nur für seinen Eigner zur Verfügung. Er ermöglicht dem Eigner das Empfangen einer privaten Transaktion oder eine digitale Unterschrift. Die mit einem privaten Schlüssel unterzeichneten Daten können nur mit dem entsprechenden öffentlichen Schlüssel geprüft werden. *Gegensatz zu* Öffentlicher Schlüssel. *Siehe auch* Schlüsselpaar aus öffentlichem und privatem Schlüssel.

Protokoll
Eine vereinbarte Konvention für die Kommunikation zwischen Computern.

Protokollierungssubsystem
Bei Tivoli PKI ein Subsystem, das die Unterstützungsfunktionen zum Protokollieren von sicherheitsrelevanten Aktionen bereitstellt. Es entspricht den Empfehlungen, die im X9.57-Standard unter *Public Key Cryptography for the Financial Services Industry* definiert wurden.

Proxy-Server
Eine Einheit, die zwischen einem Computer, der eine Zugriffsanforderung absetzt (Computer A) und einem Computer, auf den zugegriffen werden soll (Computer B), implementiert ist. Wenn ein Endbenutzer eine Anforderung für eine Ressource über Computer A absetzt, wird diese an den Proxy-Server geleitet. Dieser sendet die Anforde-

rung an Computer B, erhält von diesem die Antwort und leitet diese an den Endbenutzer weiter. Mit Hilfe eines Proxy-Servers kann über einen Computer, der sich innerhalb einer Firewall befindet, auf das World Wide Web zugegriffen werden.

Prüf-Client
Jeder Client im System, der Prüfereignisse an den Tivoli PKI-Prüf-Server sendet. Bevor ein Prüf-Client ein Ereignis an den Prüf-Server sendet, stellt er eine Verbindung zu diesem her. Nach der Herstellung der Verbindung verwendet der Client die Client-Bibliothek des Prüfsubsystems, um Ereignisse an den Prüf-Server zu übertragen.

Prüfprotokoll
Daten in Form eines logischen Pfades, die eine Folge von Ereignissen verbinden. Mit dem Prüfprotokoll können Transaktionen oder der bisherige Verlauf einer bestimmten Aktivität verfolgt werden.

Prüfprotokoll
Bei Tivoli PKI eine Tabelle in einer Datenbank, in der für jedes Prüfereignis ein Datensatz gespeichert wird.

Prüf-Server
Ein Tivoli PKI-Server, der zum Empfangen von Prüfereignissen von Prüf-Clients und zum Aufzeichnen dieser Ereignis in einem Prüfprotokoll dient.

Prüfzeichenfolge
Eine Zeichenfolge, die von einem Server oder einer Anwendung gesendet wird und zum Anfordern der Benutzerberechtigung dient. Der Benutzer, der zur Authentifizierung aufgefordert wird, unterzeichnet die Prüfzeichenfolge mit einem privaten Schlüssel. Der öffentliche Schlüssel des Benutzers sowie die unterzeichnete Prüfzeichenfolge werden zurück an den Server oder die Anwendung gesendet, der bzw. die die Authentifizierung anforderte. Der Server versucht anschließend, die unterzeichnete Prüfzeichenfolge mit Hilfe des öffentlichen Schlüssels des Benutzers zu entschlüsseln. Wenn die entschlüsselte Prüfzeichenfolge mit der ursprünglich gesendeten Prüfzeichenfolge übereinstimmt, gilt der Benutzer als authentifiziert.

Public Key Cryptography Standards (PKCS)
Informelle, herstellerübergreifende Standards, die im Jahr 1991 von den RSA Laboratories in Zusammenarbeit mit Repräsentanten verschiedener Computerhersteller entwickelt wurden. Diese Standards umfassen die RSA-Verschlüsselung, die Diffie-Hellman-Vereinbarung, die kennwortbasierte Verschlüsselung sowie die Syntax für erweiterte Zertifikate, verschlüsselte Nachrichten, Daten zu privaten Schlüsseln und für die Zertifizierung.

- PKCS #1 beschreibt ein Verfahren zum Verschlüsseln von Daten mit Hilfe des RSA-Verschlüsselungssystems auf der Basis öffentlicher Schlüssel. Er dient zur Erstellung digitaler Unterschriften und Briefumschläge.
- PKCS #7 definiert ein allgemeines Format für verschlüsselte Nachrichten.
- PKCS #10 definiert eine Standardsyntax für Zertifizierungsanforderungen.
- PKCS #11 definiert eine Programmierschnittstelle für Verschlüsselungseinheiten, z. B. Smart-Cards, die unabhängig vom verwendeten technologischen Konzept ist.
- PKCS #12 definiert ein portierbares Format zum Speichern oder Transportieren der privaten Schlüssel, Zertifikate und sonstiger geheimer Daten etc. eines Benutzers.

Public Key Infrastructure (PKI)
Ein Standard für Sicherheitssoftware, der auf der Verschlüsselung mit Hilfe öffentlicher Schlüssel basiert. Bei PKI handelt es sich um ein System digitaler Zertifikate, Zertifikatsaussteller, Registrierungsstellen, Zertifikatverwaltungsservices und verteilter Verzeichnisservices. Er dient zum Prüfen der Identität und Berechtigung aller Parteien, die an Transaktionen beteiligt sind, die über das Internet ausgeführt werden. Diese Transaktionen umfassen möglicherweise Operationen, zu deren Ausführung eine Identitätsprüfung erforderlich ist. Sie dienen z. B. zur Bestätigung des Ursprungs von Senderechtanforderungen, E-Mail-Nachrichten oder Finanztransaktionen.
PKI erreicht dieses Ziel dadurch, dass öffentliche Chiffrierschlüssel und Benutzerzertifikate für die Authentifizierung durch eine berechtigte Einzelperson oder ein berechtigtes Unternehmen verfügbar gemacht werden. Er stellt Onlineverzeichnisse bereit, die die öffentlichen Chiffrierschlüssel und Zertifikate enthalten, die zur Überprüfung der digitalen Zertifikate, Identitätsnachweise sowie der digitalen Unterschriften verwendet werden.
PKI stellt außerdem Funktionen zur schnellen und effizienten Antwort auf Prüfabfragen und Anforderungen für öffentliche Chiffrierschlüssel bereit. Der Standard dient darüber hinaus zur Identifizierung potenzieller Sicherheitslücken im System und zur Verwaltung von Ressourcen zur Bearbeitung von Sicherheitsverletzungen. PKI bietet außerdem einen digitalen Zeitmarkenservice für wichtige Unternehmenstransaktionen.

R

RA

Registration Authority - Registrierungsstelle.

RA Desktop

Ein Java-Applet, das den RAs eine grafische Oberfläche für die Verarbeitung von Anforderungen für Identitätsnachweise und zur Verwaltung dieser Nachweise während ihrer Gültigkeitsdauer zur Verfügung stellt.

RA-Server

Der Server für die RA-Komponente von Tivoli PKI.

RC2

Eine variable Schlüsselgrößen-Block-Cipher, die von Ron Rivest für RSA Data Security entwickelt wurde. *RC* steht für *Ron's Code* oder *Rivest's Cipher*. Sie arbeitet schneller als DES und löst diese Block-Cipher ab. Durch die Verwendung geeigneter Schlüsselgrößen kann sie in Bezug auf eine ausgedehnte Schlüsselsuche flexibler als DES gestaltet werden. Sie verfügt über eine Blockgröße von 64 Bit und arbeitet auf Softwareebene zwei- bis dreimal schneller als DES. RC2 kann in denselben Modi eingesetzt werden wie DES.
Durch eine Vereinbarung zwischen SPA (Software Publishers Association) und der US-Regierung nimmt RC2 einen speziellen Status ein. Hierdurch ist das Genehmigungsverfahren für den Export einfacher und schneller, als dies bei anderen Verschlüsselungsprodukten der Fall ist. Um die Voraussetzungen für eine rasche Exportgenehmigung zu erfüllen, muss ein Produkt mit einigen Ausnahmen die RC2-Schlüsselgröße auf 40 Bit beschränken. Eine zusätzliche Zeichenfolge kann verwendet werden, um Nichtberechtigte abzuwehren, die versuchen, eine umfangreiche Tabelle möglicher Verschlüsselungsvarianten vorauszuberechnen.

Regel-Exit

In einer Registrierungsfunktion ein auf Unternehmensebene definiertes Programm, das von der Registrierungsanwendung aufgerufen wird. Die Regeln eines Regel-Exits implementieren die Unternehmens- und Sicherheitsbenutzervorgaben eines Unternehmens für den Registrierungsprozess.

Registrierter Name (DN)

Der eindeutige Name eines im Directory gespeicherten Dateneintrags. Der DN dient zur eindeutigen Identifizierung der Position eines Eintrags in der hierarchischen Struktur des Directory.

Registrator

Ein Benutzer, der für den Zugriff auf RA Desktop sowie zur Verwaltung und Anforderung von Zertifikaten berechtigt ist.

Registrierung

Bei Tivoli PKI das Abrufen von Identitätsnachweisen für die Verwendung über das Internet. Bei der Registrierung werden Zertifikate angefordert, erneuert und widerrufen.

Registrierungsstelle (RA)

Die Software, die zur Verwaltung digitaler Zertifikate verwendet wird und sicherstellt, dass die Unternehmensregeln vom ersten Empfang einer Registrierungsanforderung bis zum Zertifikatswiderruf angewendet werden.

Registrierungsfunktion

Ein Tivoli PKI-Anwendungsgerüst, das spezielle Verfahren zur Registrierung von Entitäten (z. B. Browser, Router, E-Mail-Einheiten und sichere Client-Anwendungen) und zur Verwaltung von Zertifikaten während ihrer Gültigkeitsdauer bereitstellt.

Registrierungsattribut

Eine Registrierungsvariable, die in einem Registrierungsformular enthalten ist. Ihr Wert gibt die Informationen wider, die während der Registrierung erfasst werden. Der Wert des Registrierungsattributs bleibt während der gesamten Gültigkeitsdauer des Identitätsnachweises gleich.

Registrierungsdatenbank

Diese Datenbank enthält Informationen zu Zertifikatsanforderungen und ausgestellten Zertifikaten. In der Datenbank werden Registrierungsdaten gespeichert und alle Änderungen aufgezeichnet, die während der Gültigkeitsdauer an einem Zertifikat vorgenommen werden. Die Datenbank kann durch RA-Prozesse und Regel-Exits oder durch den Registrator aktualisiert werden.

Registrierungsdomäne
Eine Gruppe von Ressourcen, Regeln und Konfigurationsoptionen, die sich auf bestimmte Registrierungsprozesse für Zertifikate beziehen. Der Domänenname stellt einen untergeordneten Wert zur URL-Adresse dar, die zur Ausführung der Registrierungsfunktion eingesetzt wird.

Registrierungsprozess
Bei Tivoli PKI die Schritte, die zur Überprüfung eines Benutzers ausgeführt werden. Durch den Registrierungsprozess werden Benutzer sowie deren öffentliche Schlüssel zertifiziert, um sie zur Teilnahme an den gewünschten Transaktionen zu berechtigen. Er kann lokal oder Web-gestützt, automatisch oder von einer tatsächlich mit Personen besetzten Registrierungsstelle ausgeführt werden.

Registrierungsvariable
Siehe Registrierungsattribut.

RSA
Ein auf öffentlichen Schlüsseln basierender Verschlüsselungsalgorithmus, der nach seinen Erfindern (Rivest, Shamir und Adelman) benannt wurde. Er wird zur Verschlüsselung und für digitale Unterschriften verwendet.

S

Schema
Beim Directory die interne Struktur, die zur Definition der Beziehungen zwischen den verschiedenen Objektarten verwendet wird.

Schlüssel
Bei der Verschlüsselung ein Wert, der zum Ver- und Entschlüsseln von Informationen verwendet wird.

Schlüsselpaar
Zusammengehörende Schlüssel, die bei der asymmetrischen Verschlüsselung eingesetzt werden. Ein Schlüssel wird zur Verschlüsselung, der andere zur Entschlüsselung verwendet.

Schlüsselpaar aus öffentlichem und privatem Schlüssel
Ein Schlüsselpaar aus öffentlichem und privatem Schlüssel stellt ein grundlegendes Element der Verschlüsselung auf der Basis von Schlüsselpaaren dar. (Diese Form der Verschlüsselung wurde im Jahr 1976 von Whitfield Diffie und Martin Hellman eingeführt, um Probleme bei der Schlüsselverwaltung zu lösen.) Nach diesem Konzept erhält jeder Benutzer ein Schlüsselpaar, bei dem einer als öffentlicher und einer als privater Schlüssel bezeichnet wird. Der öffentliche Schlüssel ist hierbei allgemein bekannt, der private Schlüssel wird hingegen geheim gehalten. Sender und Empfänger müssen geheime Daten nicht gemeinsam benutzen. Alle Kommunikationsoperationen werden lediglich auf der Basis öffentlicher Schlüssel ausgeführt. Die privaten Schlüssel werden niemals übertragen oder gemeinsam verwendet. Auf diese Weise ist es nicht mehr notwendig, sich auf die Sicherheit eines Übertragungskanals gegenüber Manipulationen zu verlassen. Die einzige Anforderung ist, dass öffentliche Schlüssel den entsprechenden Benutzern in einer gesicherten (authentifizierten) Weise (z. B. in einem gesicherten Verzeichnis) zugeordnet werden. Jeder Benutzer kann nun mit Hilfe dieser öffentlichen Daten eine vertrauliche Nachricht senden. Diese Nachricht kann nur mit einem privaten Schlüssel entschlüsselt werden, auf den allein der gewünschte Empfänger zugreifen kann. Darüber hinaus kann die Verschlüsselung auf der Basis von Schlüsselpaaren nicht nur zur Gewährleistung der Vertraulichkeit (Verschlüsselung), sondern auch für die Authentifizierung (digitale Unterschriften) eingesetzt werden.

Secure Electronic Transaction (SET)
Ein Branchenstandard für die Durchführung sicherer Kredit- oder Kundenkartenzahlungen über nicht gesicherte Netze. Der Standard formuliert Definitionen für die Authentifizierung von Kartenhaltern, Händlern sowie der Banken, durch die die Karten ausgestellt werden, da er die Ausstellung von Zertifikaten anfordert.

Secure Sockets Layer (SSL)
Ein IETF-Standardübertragungsprotokoll mit integrierten Sicherheitsservices, die für den Endbenutzer möglichst transparent sind. Es stellt einen digitalen, sicheren Kommunikationskanal zur Verfügung.
Ein SSL-fähiger Server empfängt SSL-Verbindungsanforderungen im Allgemeinen an einem anderen Anschluss (Port) als normale HTTP-Anforderungen. SSL erstellt eine Sitzung, in der die Austauschsignale zum Herstellen der Kommunikation zwischen zwei Modems nur einmal gesendet werden müssen. Anschließend wird die Kommunikation verschlüsselt und die Nachrichtenintegrität wird solange überprüft, bis die SSL-Sitzung abgelaufen ist.

Server

(1) In einem Netz eine Datenstation, die anderen Stationen Funktionen zur Verfügung stellt, wie beispielsweise ein Datei-Server. (2) In TCP/IP ein System in einem Netz, das die Anforderungen eines Systems an einem anderen Standort verarbeitet. Dieses Konzept wird als Client/Server-Modell bezeichnet.

Server-Zertifikat

Ein digitales Zertifikat, das von einem CA ausgegeben wird und es einem Web-Server ermöglicht, SSL-gestützte Transaktionen auszuführen. Wenn ein Browser über das SSL-Protokoll eine Verbindung zum Server herstellt, sendet der Server seinen öffentlichen Schlüssel an den Browser. Hierdurch kann die Identität des Servers authentifiziert werden und es können verschlüsselte Daten an den Server gesendet werden. *Siehe auch* CA-Zertifikat, Digitales Zertifikat, *und* Browser-Zertifikat.

Servlet

Ein Server-Programm, das zusätzliche Funktionen für Server zur Verfügung stellt, die Java unterstützen.

SET

Secure Electronic Transaction.

SGML

Standard Generalized Markup Language.

SHA-1 (Secure Hash Algorithm)

Ein von NIST und NSA entwickelter Algorithmus, der beim DSS (Digital Signature Standard) verwendet wird. Der Standard wird als Secure Hash Standard bezeichnet; SHA ist der Algorithmus, der von diesem Standard verwendet wird. Er generiert einen 160-Bit-Hash-Code.

Sicherheitsdomäne

Eine Gruppe (z. B. Unternehmen, Arbeitsgruppe, Projektteam), deren Zertifikate vom gleichen CA zertifiziert wurden. Benutzer, die über ein von einem CA unterzeichnetes Zertifikat verfügen, können der Identität eines anderen Benutzers vertrauen, der ein Zertifikat besitzt, das vom selben CA unterzeichnet worden ist.

Sicherungsmodell

Eine Organisationskonvention, die regelt, wie Zertifikatsaussteller (CAs) andere Zertifikatsaussteller zertifizieren können.

Sicherung und Wiederherstellung von Schlüsseln

Diese Funktion von Tivoli PKI ermöglicht das Sichern und Wiederherstellen der Endentitätszertifikate sowie ihrer entsprechenden von Tivoli PKI zertifizierten öffentlichen und privaten Schlüssel. Die Zertifikate und Schlüssel werden in einer PKCS #12-Datei gespeichert. Diese Datei wird durch ein Kennwort geschützt. Das Kennwort wird zum Zeitpunkt der Sicherung der Zertifikate und Schlüssel festgelegt.

Simple Mail Transfer Protocol (SMTP)

Ein Protokoll, mit dem elektronische Post über das Internet übertragen wird.

Site-Zertifikat

Dieser Zertifikatstyp ist mit einem CA-Zertifikat vergleichbar, gilt jedoch nur für eine bestimmte Website. *Siehe auch* CA-Zertifikat.

Smart-Card

Eine Hardwarekomponente, normalerweise in der Größe einer Kreditkarte, auf der die digitalen Schlüssel eines Benutzers gespeichert werden können. Eine Smart-Card kann kennwortgeschützt werden.

S/MIME

Ein Standard, der das Unterzeichnen und Verschlüsseln von elektronischer Post (E-Mail) unterstützt, die über das Internet übertragen wird. *Siehe* MIME.

SMTP

Simple Mail Transfer Protocol.

SSL

Secure Sockets Layer.

Standard Generalized Markup Language (SGML)

Ein Standard zur Beschreibung von Formatierungssprachen. HTML basiert auf SGML.

Symmetrischer Schlüssel
Ein Schlüssel, der sowohl für die Verschlüsselung als auch für die Entschlüsselung verwendet werden kann. *Siehe auch* Symmetrische Verschlüsselung.

Symmetrische Verschlüsselung
Eine Form der Verschlüsselung, bei der sowohl für die Ver- als auch für die Entschlüsselung derselbe Schlüssel verwendet wird. Die Sicherheit dieses Verfahren basiert auf dem Schlüssel. Wird dieser öffentlich bekannt gegeben, können die mit ihm bearbeiteten Nachrichten von jedem Benutzer ver- und entschlüsselt werden. Der Inhalt der übertragenen Daten kann nur dann geheim gehalten werden, wenn der Schlüssel nur den jeweils berechtigten Personen bekannt ist. *Gegensatz zu* Asymmetrische Verschlüsselung.

T

TCP/IP
Transmission Control Protocol/Internet Protocol.

Tivoli PKI
Eine integrierte IBM SecureWay-Sicherheitslösung, die die Ausstellung, die Erneuerung und den Widerruf digitaler Zertifikate unterstützt. Diese Zertifikate können für eine breite Palette von Internet-Anwendungen eingesetzt werden und bieten eine Möglichkeit zur Authentifizierung von Benutzern und zur Gewährleistung einer gesicherten Kommunikation.

TP
Trust Policy = Sicherungsregel.

Transaktions-ID
Eine Kennung, die die RA als Antwort auf eine Anforderung für eine Vorabregistrierung zur Verfügung stellt. Mit dieser ID kann ein Benutzer, der die Client-Anwendung von Tivoli PKI ausführt, ein vorab genehmigtes Zertifikat erhalten.

Transmission Control Protocol/Internet Protocol (TCP/IP)
Eine Gruppe von Übertragungsprotokollen, die Peer-zu-Peer-Konnektivitätsfunktionen für lokale Netze (LANs) und Weitverkehrsnetze (WANs) unterstützen.

Triple DES
Ein symmetrischer Algorithmus, bei dem der unverschlüsselte Text dreimal verschlüsselt wird. Obwohl für diese Mehrfachverschlüsselung zahlreiche Methoden existieren, stellt die Triple DES-Verschlüsselung, die auf drei verschiedenen Schlüsseln basiert, das sicherste dieser Verfahren dar.

Trust-Kette
Eine Gruppe von Zertifikaten, die aus der gesicherten Hierarchie besteht, die sich vom Benutzerzertifikat bis hin zur Root bzw. dem selbst unterzeichnenden Zertifikat erstreckt.

Tunnel
In der VPN-Technologie eine virtuelle Punkt-zu-Punkt-Verbindung, die auf Anfrage über das Internet hergestellt wird. Während der Verbindung können ferne Benutzer den Tunnel verwenden, um sichere, verschlüsselte und gekapselte Informationen mit Servern im privaten Netz eines Unternehmens auszutauschen.

U

Unbestreitbarkeit
Die Verwendung eines digitalen, privaten Schlüssels, um zu verhindern, dass der Unterzeichner eines Dokuments dessen Unterzeichnung leugnet.

Unicode
Ein 16-Bit-Zeichensatz, der in ISO 10646 definiert ist. Der Unicodestandard für die Verschlüsselung von Zeichen ist ein internationaler Zeichencode für die Informationsverarbeitung. Er umfasst die grundlegenden, weltweit verwendeten Prozeduren und bildet die Basis für die Internationalisierung und Lokalisierung von Software. Der gesamte Quellcode in der Java-Programmierungsumgebung wird in Unicode geschrieben.

Unternehmensprozessobjekte
Eine Codegruppe, die zur Ausführung einer bestimmten Registrierungsoperation, z. B. zum Prüfen des Registrierungsstatus oder zur Bestätigung des Sendens eines öffentlichen Schlüssels, verwendet wird.

Unternehmensprozessschablone
Eine Gruppe von Unternehmensprozessobjekten, die in einer bestimmten Reihenfolge ausgeführt werden.

Unterstützung in der Landessprache (NLS)
Unterstützung für unterschiedliche länderspezifische Angaben in einem Produkt. Hierzu gehören die Sprache, die Währung, das Datums- und Zeitformat und die Darstellung von Zahlen.

Unterzeichnen
Die Verwendung eines digitalen privaten Schlüssels zum Generieren einer Unterschrift. Diese Unterschrift dient dazu, zu beweisen, dass ein bestimmter Benutzer für die von ihm unterzeichnete Nachricht verantwortlich ist und diese akzeptiert.

Unterzeichnen/Prüfen
Als Unterzeichnen wird die Verwendung eines privaten Schlüssels zum Generieren einer Unterschrift bezeichnet. Unter Prüfen versteht man die Verwendung des entsprechenden öffentlichen Schlüssels zur Verifizierung dieser Unterschrift.

Unverschlüsselter Text
Nicht verschlüsselte Daten. *Synonym zu* Klartext.

URL
Uniform Resource Locator - URL-Adresse.

URL-Adresse
Ein Schema für die Adressierung von Ressourcen im Internet. Die URL-Adresse gibt das verwendete Protokoll sowie den Host-Namen und die IP-Adresse an. Außerdem enthält er Angaben zur Anschlussnummer, zum Pfad sowie weitere Ressourcendetails, die erforderlich sind, um über eine bestimmte Maschine auf eine Ressource zuzugreifen.

UTF-8
Ein Umsetzungsformat. Es ermöglicht Informationsverarbeitungssystemen, die nur die Verarbeitung von 8-Bit-Zeichensätzen unterstützen, die Umsetzung von 16-Bit-Unicode in ein 8-Bit-Äquivalent und umgekehrt, ohne dass hierbei Informationen verloren gehen.

V

Verkettungsprüfung
Die Gültigkeitsprüfung aller CA-Unterschriften in der Trust-Hierarchie, über die ein bestimmtes Zertifikat ausgestellt wurde. Wenn z. B. das Unterschriftszertifikat eines CA über einen anderen CA ausgestellt wurde, werden bei der Gültigkeitsprüfung des vom Benutzer vorgelegten Zertifikats beide Unterschriften geprüft.

Verschlüsseln
Das Umordnen von Informationen, so dass nur Personen, die über den richtigen Entschlüsselungscode verfügen, die ursprünglichen Informationen durch Entschlüsselung abrufen können.

Verschlüsselt
Die Eigenschaft von Daten, die nach einem bestimmten System umgesetzt wurden, um deren Bedeutung unkenntlich zu machen.

Verschlüsselung/Entschlüsselung
Die Verwendung des öffentlichen Schlüssels des gewünschten Empfängers zum Verschlüsseln von Daten für diese Person. Der Empfänger verwendet anschließend den privaten Schlüssel seines Schlüsselpaares, um die Daten zu entschlüsseln.

Vertrauensdomäne
Eine Gruppe von Entitäten, deren Zertifikate vom gleichen CA zertifiziert wurden.

Vertraulichkeit
Der Schutz von Daten gegen den Zugriff nicht berechtigter Personen.

Vertraulichkeit
Die Wahrung der Geheimhaltung bestimmter Informationen gegenüber nicht berechtigten Personen.

Virtual Private Network (VPN)
Ein privates Datennetz, das ferne Verbindungen nicht über Telefonleitungen, sondern über das Internet herstellt. Da der Zugriff der Benutzer auf die Netzressourcen eines Unternehmens nicht über eine Telefongesellschaft, sondern über einen Internet Service Provider (ISP) erfolgt, können diese durch den Einsatz von VPN deutliche Einsparungen bei Fernzugriffen erzielen. Ein VPN erhöht auch die Sicherheit beim Datenaustausch. Bei der herkömmlichen Firewall-Technologie kann zwar der Inhalt der Nachricht verschlüsselt werden, nicht jedoch die Quellen- und Zieladressen. Bei der VPN-Technologie können die Benutzer eine Tunnelverbindung herstellen, bei der das gesamte Datenpaket (Header- und Datenkomponente) verschlüsselt und gekapselt ist.

Vorabregistrierung
Bei Tivoli PKI ein Prozess, mit dem ein bestimmter Benutzer (normalerweise ein Administrator) andere Benutzer registrieren kann. Wenn die Anforderung genehmigt wird, stellt die RA Informationen zur Verfügung, mit denen der Benutzer später mit Hilfe der Client-Anwendung von Tivoli PKI ein Zertifikat erhalten kann.

VPN
Virtual Private Network.

W

Web-Browser
Auf einem PC ausgeführte Client-Software, mit der ein Benutzer im World Wide Web navigieren oder lokale HTML-Seiten anzeigen kann. Der Web-Browser ist ein Abfrage-Tool, das universellen Zugriff auf die umfangreichen Hypermedia-Datensammlungen ermöglicht, die im Web und im Internet zur Verfügung gestellt werden. Manche Browser können Text und Grafik anzeigen, während andere Browser auf die Textanzeige beschränkt sind. Die meisten Browser unterstützen die Hauptformen der Internet-Kommunikation, z. B. die Ausführung von FTP-Transaktionen.

Web-Server
Ein Server-Programm, das auf Anforderungen von Browser-Programmen nach Informationsressourcen antwortet. *Siehe auch* Server.

WebSphere Application Server
Ein IBM Produkt, das Benutzer bei der Entwicklung und Verwaltung von Websites mit einem hohen Leistungsumfang unterstützt. Es erleichtert den Übergang vom einfachen Web Publishing zu komplexen e-business-Anwendungen im Web. Der WebSphere Application Server besteht aus einer Java-Servlet-Maschine, die unabhängig vom Webserver und dem verwendeten Betriebssystem arbeitet.

World Wide Web (WWW)
Der Teil des Internets, in dem ein Netz von Verbindungen zwischen Computern aufgebaut wird, auf denen Hypermediamaterial gespeichert ist. Dieses Material stellt neben Informationen auch Verbindungen (Hyperlinks) zu anderem Material im World Wide Web und Internet zur Verfügung. Der Zugriff auf WWW-Ressourcen erfolgt über einen Web-Browser.

X

X.500
Ein Standard für die Implementierung eines multifunktionalen, verteilten und vervielfältigten Verzeichnisservices durch die Verbindung von Computersystemen. Dieser Standard wurde gemeinsam definiert von der bisher als CCITT bekannten International Telecommunications Union (ITU) sowie der International Organization for Standardization und der International Electro-Chemical Commission (ISO/IEC).

X.509 Version 3-Zertifikat
Das X.509v3-Zertifikat verfügt über erweiterte Datenstrukturen für die Speicherung und das Abrufen von Informationen zu Zertifikatsanträgen, zur Zertifikatsverteilung und zu Zertifikatswiderrufen sowie zu Sicherheitsregeln und digitalen Unterschriften.
X.509v3-Prozesse dienen zum Erstellen von CRLs mit Zeitmarken für alle Zertifikate. Bei jeder Verwendung eines Zertifikats ermöglichen die X.509v3-Funktionen der Anwendung, die Gültigkeit des Zertifikats zu überprüfen. Die Anwendung kann außerdem feststellen, ob sich das Zertifikat auf der Zertifikatswiderrufsliste (CRL) befindet. CRLs unter X.509v3 können für einen bestimmte Gültigkeitszeitraum erstellt werden. Sie können auch

auf anderen Kriterien basieren, die zur Aufhebung der Gültigkeit eines Zertifikats führen. Wenn z. B. ein Mitarbeiter ein Unternehmen verlässt, wird sein Zertifikat in der CRL eingetragen.

X.509-Zertifikat
Ein weit verbreiteter Zertifikatsstandard, der entwickelt wurde, um die sichere Verwaltung und Verteilung von digital unterzeichneten Zertifikaten über sichere Internet-Netze zu unterstützen. Das X.509-Zertifikat definiert Datenstrukturen, die Prozeduren für die Verteilung öffentlicher Schlüssel unterstützen, die von zuverlässigen Stellen digital unterzeichnet sind.

Z

Zertifikatsaussteller (CA)
Die Software, die zur Einhaltung der Sicherheitsregeln eines Unternehmens und zur Vergabe gesicherter elektronischer Identitäten in Form von Zertifikaten dient. Der CA verarbeitet die Anforderungen von RAs zum Ausstellen, Erneuern und Widerrufen von Zertifikaten. Er kooperiert mit der RA, um Zertifikate und CRLs im Directory zu veröffentlichen. *Siehe auch* Digitales Zertifikat.

Zertifikatserweiterung
Eine Zusatzfunktion des X.509v3-Zertifikatformats, die zur Einbindung zusätzlicher Felder in das Zertifikat dient. Es stehen Standard- und benutzerdefinierte Erweiterungen zur Verfügung. Die Standarderweiterungen dienen verschiedenen Zwecken und umfassen Schlüssel- und Regelinformationen, Betreff- und Ausstellerattribute sowie Einschränkungen, die für den Zertifizierungspfad gelten.

Zertifikatsprofil
Eine Gruppe von Kenndaten, die den gewünschten Zertifikatstyp definieren (z. B. SSL- oder IPSec-Zertifikate). Das Profil vereinfacht die Zertifikatsspezifikation und -registrierung. Der Aussteller kann die Namen der Profile ändern und Kenndaten des gewünschten Zertifikats angeben. Hierzu zählen z. B. der Gültigkeitszeitraum, die Verwendung von Schlüsseln, DN-Einschränkungen usw.

Zertifikatsregel
Eine benannte Gruppe mit Regeln, die angibt, ob ein Zertifikat für eine bestimmte Klasse von Anwendungen mit gemeinsamen Sicherheitsanforderungen anwendbar ist. Eine Zertifikatsregel kann z. B. angeben, ob ein bestimmter Zertifizierungstyp dem Benutzer die Ausführung von Transaktionen für Waren innerhalb eines bestimmten Preisbereichs ermöglicht.

Zertifikatswiderrufsliste (CRL)
Eine digital unterzeichnete, mit Zeitmarken versehene Liste der Zertifikate, die vom Zertifikatsaussteller (CA) widerrufen wurden. Die Zertifikate in dieser Liste sollten als nicht akzeptierbar behandelt werden. *Siehe auch* Digitales Zertifikat.

Zertifizierung
Der Prozess, bei dem eine zuverlässige, an der Kommunikation nicht beteiligte Stelle (der Zertifikatsaussteller - CA) einen elektronischen Identitätsnachweis ausstellt, der für die Identität einer Person, eines Unternehmens oder einer Organisation bürgt.

Ziel
Eine benannte oder ausgewählte Datenquelle.

Zugriffssteuerungsliste (ACL)
Ein Verfahren, mit dem die Verwendung einer bestimmten Ressource auf berechtigte Benutzer beschränkt werden kann.

Index

A

Abfrage
- ablaufende Zertifikate 14
- anhand von Anforderungsstatus 40
- anhand von Schlüsselwiederherstellungsstatus 41
- anstehende Anforderungen 13
- Felder 39
- nach Erneuerbarkeit 42
- Rückmeldungen bei Verarbeitung 15
- Servlet zur Unterstützung 36
- überarbeiten 15
- übergeben 12
- vorbereiten 12
- vordefiniert 43

Abfrage, Registerkarte 39
Abfrageergebnisse
- ablaufende Zertifikate 14
- Aktionen ausführen für 20, 21, 24, 25, 26
- Aktionsprotokoll anzeigen 18
- als Liste anzeigen 15, 44
- anstehende Anforderungen 13
- Anzahl der abzurufenden Datensätze definieren 15, 43
- anzeigen 15
- Attribute anzeigen 17
- Datensätze auswählen 20
- Details anzeigen 17
- durchblättern 17
- Sätze pro Seite begrenzen 15
- Schlüsselwiederherstellung 13

Ablaufdatum von Zertifikaten 14, 22
Aktion des Registrators
- Anforderung genehmigen 24
- Anforderung im Status ″anstehend″ behalten 24
- Anforderung zurückweisen 24
- Anforderungsprofil definieren 23
- Attribute ändern 17
- Erneuerbarkeit ändern 25
- Gültigkeitszeitraum ändern 22
- Kommentar hinzufügen 23
- Rückmeldungen abrufen 15
- Schlüsselwiederherstellungsanforderung genehmigen 24
- Schlüsselwiederherstellungsanforderung zurückweisen 25
- Zertifikat widerrufen 26
- Zertifikate publizieren 27
- zulässig für Domäne 27, 45

Aktionsprotokoll
- anzeigen 18
- Ereignisse 47
- Spalten in Tabelle 46

Aktivieren ausgesetzter Zertifikate 26
Anforderungs-ID 7, 9
Anforderungsattribute 47
Anforderungsprofil 23, 37
Anstehende Anforderung für Schlüsselwiederherstellung abrufen 13
Anzahl der abzurufenden Datensätze
- definieren 15
- Optionen 44

Attribute, Datenbanksatz 32
Attribute, Zertifikat und Anforderung
- ändern 17
- anzeigen 17
- für Anforderung oder Zertifikat 47
- Unternehmensprozessvariablen 22
- Werte ändern 22
- Zertifikatserweiterungen 49

Aussetzen von Zertifikaten 25, 35
Aussetzen von Zertifikats 46
Authentifizierung 36

B

Beenden von RA Desktop 27
Berechtigung für Registrator 10
Berechtigungen 45
- für Aktion in Domäne 20, 27
- für Domäne abrufen 10
- für Domäne prüfen 27

Bibliothek, Tivoli PKI-Website ix
Browser 6
- Szenario für Vorabregistrierung 29
- unterstützte 30
- URL-Adresse 6
- Vorbereitung 5, 6

Browser-Unterstützung 30
Browser-Zertifikat 7, 12, 33

C

CA-Hierarchie 32
CA-Zertifikat 7, 34
CRL, Zertifikat wieder aufnehmen 26

D

Dateiberechtigungen, Registrator 10, 20, 21
Datenbanksätze
- Abfrage begrenzen 15
- abfragen 12
- Attribute 32
- Felder zum Abrufen 39

Datenbanksätze *(Forts.)*
für Aktionen auswählen 20
Sätze pro Seite definieren 15
Verarbeitung durch RA 3
vordefinierte Abfrage 43
Datensätze auswählen 20
Datumsangabe angeben 14
DB2 31
Deinstallieren von RA Desktop 28
Details, Registerkarte 46
Directory-Zugriff 33
Domäne, Registrierung 31

E

E-Mail-Benachrichtigung 7
Einheitenzertifikat 34
Entfernen von RA Desktop 28
Ergebnisse, Registerkarte 44
Sätze pro Seite 15
Seiten anzeigen 17
Erläuterungen, Abschnitte 29
Erneuerbarkeit 25, 35

F

Felder, RA Desktop
auf der Registerkarte 'Ergebnisse' 45
auf Registerkarte Abfrage 39
auf Registerkarte Details 46
Hilfe für 52
Feldhilfe 52

G

Gegenseitige Zertifizierung 32
Gründe für Widerruf 46
Gültigkeitszeitraum 22, 37, 49

H

Hilfe für RA Desktop 39

I

Identifikationsprüfungsantwort 7, 9
Informationen zur Vorgehensweise, Abschnitte 5
Inhalt des Handbuchs ix
Installieren von RA Desktop 10
Internet Explorer
Release 52
Standardzertifikat 12

K

Kalender 14
Karenzzeit, Zertifikat 35
Konventionen xi
Kundenunterstützung xi

L

LDAP-Protokoll 33

M

Manipulierte Schlüssel 46
Mehrere Registratoren 36

P

PKCS #10-Zertifikatsanforderung 34
PKIX-kompatible Anwendungen 33
Profil, Anforderung 23, 37
Protokoll, Directory-Zugriff 33
Protokolle 33
Publizieren von Zertifikaten 27, 36

R

RA Desktop
beenden 27
Berechtigung 10
deinstallieren 28
installieren 10
Registrierung für Zugriff 7
rekonfigurieren 11
Servlet zur Unterstützung 36
Zugriff 12
Zugriff vorbereiten 5
Reaktivieren von Zertifikaten 46
Referenzabschnitte 39
Registerkarten, RA Desktop
Abfrage, Registerkarte 12, 39
allgemeine Merkmale 52
Details, Registerkarte 17
Ergebnisse, Registerkarte 15, 44
Hilfe für 52
Registerkarte 'Details' 46

Registerkarten, RA Desktop *(Forts.)*
wechseln 19
Registerkartenhilfe 52
Registrator
Aktionen 45
Aktionsprotokoll 18, 47
Auswirkung auf Registrierungsdatenbank 32
automatisierte Aufgaben 3, 30
Berechtigungen für Domäne 27, 45
Kommentar zu Aktion 23
mehrere Registratoren 36
registrieren 7
Registrierungsstatus prüfen 9
Rolle 3
Servlet zur Unterstützung von Aufgaben 36
Zertifikat für Zugriff auf RA Desktop 7
Registrierter Name 33
Registrierung 30
Aktionen 45
Anforderung 3
Aufgaben, Registrator 3
automatisiert 3, 30
Regeln 31
Unternehmensregeln anwenden 30
Web-Browser-Unterstützung 30
Registrierungs-Web-Seite
CA-Zertifikat für Verwendung 7, 34
Verwendung 29
Zugriff 6
Registrierungsanforderung
Aktionsprotokoll 47
Anforderungsstatus prüfen 9
anstehend 13
auswerten 30
automatische Auswertung 30
Datenbanksatz 32
Felder zum Abrufen 39
Registrierungsformular 29
Status 51
Verarbeitung durch RA 3, 20
von Registrator 7
Vorabregistrierung 29
Web-Browser-Unterstützung 30
Registrierungsanforderung, Gültigkeitsdauer 32
Registrierungsattribute 47
Registrierungsdatenbank 3, 31
Registrierungsdomäne 7, 10, 31, 36
Registrierungssätze 32
Abfrage begrenzen 15
abfragen 12
Attribute 32
Felder zum Abrufen 39
für Aktionen auswählen 20
Sätze pro Seite definieren 15
Verarbeitung durch RA 3
vordefinierte Abfrage 43
Registrierungsstelle 31
Rekonfigurieren von RA Desktop 11
Rückmeldungen bei Verarbeitung 15

S

Sätze pro Seite, Registerkarte 'Ergebnisse' 15, 43, 44
Schlüssel, manipuliert 46
Schlüssel, Sicherung 35
Schlüssel, Wiederherstellung 35
Schlüsselwiederherstellung 13
Seitengröße für Ergebnisse
definieren 15
Optionen 44
Server-Zertifikat 34
Servlet zur Unterstützung von RA Desktop 36
Sichere Anwendungen 3
Sicherung, Schlüssel 35
Spaltenüberschriften
Aktionsprotokolltabelle 18
Attributtabelle 17
Tabelle für Abfrageergebnisse 15
Spaltenwerte
Aktionsprotokolltabelle 46, 47
Attributtabelle 46, 47
Tabelle für Abfrageergebnisse 44
Starten von RA Desktop 12
Status
aktuell 39, 51
anzeigen 17
Werte 51
Statusbalken 52
Statusbereich 52

T

Tabelle
Abfrageergebnisse 15, 44
Aktionsprotokoll 18, 47
Attribute 17, 47
Datensätze auswählen 20
durchblättern 17
Spaltengröße anpassen 19
Zeilen sortieren 20
Tabellensätze auswählen 20
Tastatur, Alternativen zur Bedienung mit der Maus 53
Tivoli
Kundenunterstützung xi
Sicherheitsverwaltung - Webinformationen xi
Tivoli PKI
Webinformationen xi
Typ des Zertifikats 49

U

Übersicht
Registratorrolle 3
Tivoli PKI 1
Unternehmensprozessvariablen 22
Unterstützung für Tivoli-Kunden xi

URL-Adresse
Registrierungs-Web-Seite 6
Registrierungsdomäne 31
URLs
Tivoli PKI-Bibliotheksseite ix
Tivoli PKI-Homepage ix

V

Verarbeitungsattribute 47
Veröffentlichungen
beschrieben ix
Tivoli-Sicherheitsprodukte xi
Vorabregistrierung 29
Szenario für Aufgaben 29
Vorbereitung für die Verwendung von RA Desktop 5
Vorwort ix

W

Web-Browser 6
Szenario für Vorabregistrierung 29
unterstützte 30
URL-Adresse 6
Vorbereitung 5, 6
Web-Browser-Unterstützung 29, 30
Web-Seite, Registrierung
CA-Zertifikat für Verwendung 7, 34
Verwendung 29
Zugriff 6
Website für
Sicherheitsverwaltungsinformationen xi
Tivoli-Kundenunterstützung xi
Tivoli Public Key Infrastructure xi
Tivoli-Sicherheitsprodukte xi
Widerrufgründe 46
Wiederaufnehmen von Zertifikaten 35, 46
Wiederherstellung von Schlüsseln 13

X

X.509v3-Zertifikatserweiterungen 34

Z

Zertifikat 33
ablaufend 14
Aktionsprotokoll 18, 47
Anforderung 3
anstehende Anforderung 13
aussetzen 25
Datenbanksatz 31
Zertifikat *(Forts.)*
Details 46
Erneuerbarkeit 25, 34, 35
für Browser anfordern 7
Gültigkeitszeitraum 22
Kategorien 33
kontinuierliche Verwaltung 36
publizieren 27, 36
registrierter Name 33
Status 51
Typen 49
vorlegen 12
wieder aufnehmen 26
zur Ausführung von RA Desktop 7
zur Verwendung der Registrierungsservices 7, 34
Zertifikat, Gültigkeitsdauer 32, 34
Zertifikatsattribute 17, 47
Zertifikatsaussteller 32
Zertifikatserweiterungen 34, 49
Zertifikatstyp 49
Zertifikatswiderrufsliste 32
Zertifizierung 32
gegenseitige Zertifizierung 32
Hierarchie 32
Zielgruppe ix
Zugreifen auf RA Desktop 12
Zugriff auf RA Desktop 5
Zugriffssteuerungsliste 36
Zusammenfassung
verwendete Konventionen xi
Zweck des Zertifikats 49

SH12-2977-02